

LOGRHYTHM ELASTIC INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validates that security tools are writing log events to LogRhythm Elastic to ensure compliance with security policies and regulations
- Collects events generated by security tools that write to LogRhythm Elastic to test the efficacy and configuration of security controls using Security Validation jobs

Use this document to configure the integration using one of the following methods:

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

Configure MSI Integration



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

API Calls

API	Usage
<code>/_search</code>	Query for events from LogRhythm Elastic
<code>/_nodes</code>	Used to test connectivity and authentication settings

Supported Versions

- LogRhythm Elasticsearch 7.2.x
- LogRhythm Elasticsearch 7.3.x

Before You Begin

To configure this integration, you need:

- A valid username and password for a user with permissions to use the API endpoints described in the previous step
- The hostname or IP address of your LogRhythm Elastic instance

Configure Security Validation

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > LogRhythm Elastic**.



You can add this as either a Direct or Remote Integration.

3. Enter a meaningful **Integration Name**.
4. Optional: From the **Proxy** drop-down, choose a proxy profile if one is available. If one isn't available and all outbound connections go through a proxy, first, set up a **Proxy Rule** (<https://docs.mandiant.com/home/msv-proxy-rules>).
5. Change the **HttpProtocols** to use for requests. (**Https** or **Http**.)
6. For the **Host**, enter the hostname of your LogRhythm Elastic instance.
7. Enter a **Port** value. The default is **443**.
8. Enter the **Username** and **Password** for the user account with permissions to use API endpoints.
9. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).

10. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
11. Optional: Change the **Page Size** for each request to the upstream server. The default is **500**.
12. Optional: Add or remove **Queries**, as needed. Default values are provided.
13. Optional: Modify the **Max Pages** to change the maximum number of calls to the upstream server. The default is **100**.
14. Optional: Modify the **Field Map** values, as necessary.



- Each field map box can hold a JSON-formatted comma-separated list of columns returned by the API to be considered for each field when translating into the normalized event object format. Example: description could be configured to be 'msg_s' or 'SyslogMessage' in some environments. The field map tries both if set to: ['msg_s','SyslogMessage'] and whichever matches first is the column that is used.
- When configuring an integration in Security Validation, you can assign additional host values in the Field Map settings. If none of the assigned fields return a valid host name, Network Actions may miss matched events from the third-party technology. Additional hosts values helps ensure the likelihood of a match between the two environments.

15. Optional: Expand **Advanced options** and update the information as necessary.
 - a. Update **Query Time** and **Delay Time**.



The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.



If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

- b. Update **Query Interval** (seconds).
- c. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
- d. Modify the **Correlation Query Interval**, if necessary (minutes).
- e. Select **Discover network devices automatically**, the default and recommended option.




If unselected, reported events won't include product information for any matching network security technology.

- f. Select **Save Suspicious Events**.
- g. Modify the **Event Time Adjustment** (seconds). The default is **0**.
- h. Modify the **Limit** value if you need to prevent a flood of results. This value is set to **10000** by default. This limit applies to both events and alerts individually, so if you set it to **10**, you can still see a maximum of 10 events and 10 alerts.

16. Click **Save**.

Verify connectivity

1. Go to **Settings > Integrations**.
2. From the Direct Integrations table, click  > **Test** to verify that:
 - The Director can communicate with the integration host on the port and protocol specified.
 - The integration credentials are valid and working.

For more information on setting up queries, see [Manage Integrations \(https://docs.mandiant.com/home/msv-managing-integrations\)](https://docs.mandiant.com/home/msv-managing-integrations).

Configure Legacy Integration

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 \(https://docs.mandiant.com/home/msv-integrations-overview\)](https://docs.mandiant.com/home/msv-integrations-overview).



This integration is remote capable.

Update LogRhythm Elasticsearch

Prerequisites

1. Ensure network connectivity between the DX and the Security Validation Director.
2. Identify the IP address used to access Elasticsearch. This could be direct access to an Elasticsearch node, Primary node, or something such as an nginx reverse proxy.

Configuration

Complete the following steps on the LogRhythm Server (if single-tiered deployment) or DX (administrative access not required).

On the LogRhythm Server

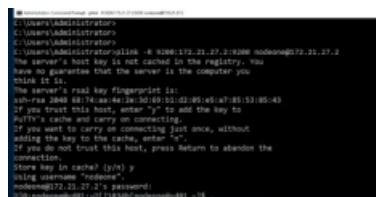
SSH from the LogRhythm DX to the Validation Platform Director.

- On a Microsoft^(R) Windows^(R) host, plink.exe can be used as follows:

```
plink -R 9200:localhost:9200 nodeone@DIRECTORIP
```

- If linux DX, use normal ssh instead of plink:

```
ssh -N -R 9200:localhost:9200 nodeone@DIRECTORIP
```



```
C:\Users\Administrator> plink -R 9200:localhost:9200 nodeone@172.21.27.2
C:\Users\Administrator>
C:\Users\Administrator> plink -R 9200:localhost:9200 nodeone@172.21.27.2
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's read key fingerprint is:
SHA-256:868 6874:86:46:14:5d:69:01:02:80:e0:a7:85:53:80:43
If you trust this host, enter "Y" to add the key to
your cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "y".
If you do not trust this host, press Return to abandon the
connection.
Want to see the full key fingerprint?
[yes/no] y
nodeone@172.21.27.2's password:
nodeone@172.21.27.2:~$
```

(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12ecc9cba0017c2f7ea1/n/lge-step1.png>)

SSH from LogRhythm to the Validation Platform Director

On the Validation Platform Director (CLI)

1. SSH to the Security Validation Director using the "nodeone" password.

a. `ssh nodeone@DIRECTOR_IP`

```
[nodeone@vd01 ~]$ ssh nodeone@172.21.16.150  
53 Connection to 172.21.16.150 closed.  
[nodeone@vd01 ~]$ ssh nodeone@172.21.27.2  
44 nodeone@172.21.27.2: password:  
[nodeone@vd01 ~]$  
etc/logstash/conf.d#
```

(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12eac9cba0017c2f7e93/n/lge-step2.png>)

SSH to the Validation Platform Director using nodeone password

2. Assume root access.

a. `sudo su -`

```
[nodeone@vd01 ~]$ sudo su -  
[sudo] password for nodeone:  
Last login: Thu Apr 26 18:36:49 UTC 2018 on pts/0  
[root@vd01 ~]#  
etc/logstash/conf.d#
```

(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12ebc9cba0017c2f7e98/n/lge-step3.png>)

Assume root access

3. Add the following custom iptables rule to allow communication to Elastic over the SSH tunnel:

a. `iptables -A INPUT -p tcp -s 127.0.0.1 --dport 9200 -j ACCEPT`

```
[root@vd01 ~]#  
[root@vd01 ~]# iptables -A INPUT -p tcp -s 127.0.0.1 --dport 9200 -j ACCEPT  
[root@vd01 ~]#  
etc/logstash/conf.d#
```

Add iptables Rules

4. Add the following configuration lines to `/etc/ssh/sshd_config`.

a. `TCPKeepAlive yes`

b. `ClientAliveInterval 15`

```
[root@vd01 ~]# echo "TCPKeepAlive yes" >> /etc/ssh/sshd_config  
[root@vd01 ~]# echo "ClientAliveInterval 15" >> /etc/ssh/sshd_config
```

Configure Keepalive

5. Restart the SSH service.

`service sshd restart`

```
[root@vd01 ~]# service sshd restart
Redirecting to /bin/systemctl restart sshd.service
[root@vd01 ~]# █
```

(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12efc9cba0017c2f7ec7/n/lge-step6.png>)

Restart SSH service

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Identify the port for Elasticsearch communication (default is 9200).
2. Identify whether the protocol is HTTP or HTTPS for connections to the Elasticsearch port.
3. Identify the field name mappings for the following (there could be multiple of each, depending on log sources and configuration):
 - Source IP
 - Destination IP
 - Source Port
 - Destination Port
 - Event Start Time (timestamp)
 - Event Unique ID
 - Event Signature ID
 - Event Description
 - Event Source Host

Configuration

TO ADD THE LOGRHYTHM ELASTICSEARCH INTEGRATION

1. Go to **Settings > Integrations**.
2. Click **Add Integration > LogRhythm Elasticsearch**.


Add LogRhythm Elasticsearch

Host*	<input type="text" value="Host"/>
Port*	<input type="text" value="Port"/>
Protocol*	<input type="text" value="https"/>
Username*	<input type="text" value="Username"/>
Password*	<input type="password" value="Password"/>
Version	<input type="text" value="7.3.x"/>
Query*	<pre>{ "stored_fields": ["normalDate", "impactedHostName", "originHostName", "impactedIp", "originIp", "impactedPort", "originPort", "logMessage", "logDate", "commonEventName", "msgSourceTypeName", "logSourceName", "query": { "bool": { "must": [{ "range": { "normalDate": { "gte": "2023-01-01T00:00:00Z", "lte": "2023-01-01T00:00:00Z" } } }] } } } }</pre>


[Show default query](#)

LogRhythm Elasticsearch Integration

3. Enter the **Host**.

 This will almost always be either "localhost" or "127.0.0.1".

4. Enter the **Port**, **Protocol**, and if using, the **Username** and **Password**.
5. Select the appropriate version.

 This may adjust the default query and field name mapping section.

6. Review and update the **Query**, if necessary.
7. Expand **Advanced options**.



(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12dec9cba0017c2f7e24/n/logrhythm-elasticsearch-advanced.png>)

LogRhythm Elasticsearch Integration (Advanced Options)

8. (Optional) Update **Query time** and **Delay time**.



The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.



If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

9. (Optional) Enable the special query for Host CLI Actions and review the **Query**.



If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

10. (Optional) Select **Discover network devices automatically**.
11. Review and update the field name mapping section.
 - a. Inputs are enclosed by square brackets `[]`.
 - b. Inputs point to the path location (`["_id"]`).
 - c. Nested locations should be enclosed in one set of brackets, encompassed in quotes, and separated by commas (`["_source", "src_ip"]`).
12. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
13. (Optional) Assign a **Name**.
14. (Optional) Choose **Yes** to save suspicious events.
15. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO LOGRHYTHM ELASTICSEARCH

Click **Test** to verify that:

- The Director can communicate with the Elasticsearch host IP address on the port specified.
- The Elasticsearch credentials can perform queries on the index or indexes with relevant data.

Updating the Integration

If you update LogRhythm, you will need to update the integration within the Validation Platform. Modifying the version may adjust the default query and the field name mapping section.

Any changes you made previously to the query and field mapping will be retained. Review the default query and the field name mapping sections to verify that no additional changes are required.