GUIDE

STORMSHIELD LOG SUPERVISOR

ALERTS AND INCIDENTS GUIDE

Version 2

Document last updated: July 4, 2024

Reference: sls-en_alerts_incidents_gde

Table of contents

Change log

Date	Description
July 4, 2024	New document

Getting started

Welcome to the SLS version 2 Alerts and Incidents Guide.

Alerts in SLS are warnings generated to notify users when any significant events occur. They fire **incidents** that enable you to execute appropriate actions. Any valid search query can trigger an alert to generate incidents. You can create an alert rule and select the medium to notify you of the incident.

Incidents are used to identify, analyze, correct, and thereby prevent information hazards in the future.

The guide provides you information on creating, managing, and customizing various rules in SLS. These rules trigger warnings as notification to users when any significant events occur. The guide serves you in learning a step-by-step execution of one or more of the following tasks.

In this document, Stormshield Log Supervisor is referred to in its short form SLS. Images used in this document are from the partner vendor's (Logpoint) software program. In your SLS, the graphics may vary but user experience is exactly the same.

Alerts

Alerts in SLS are warnings generated to notify users when any significant events occur. They fire **incidents** that enable you to execute appropriate actions. Any valid search query can trigger an alert to generate incidents.

You can create an alert rule and select the medium to notify you of the incident. SLS can notify you via e-mail, SSH, SNMP, HTTP, or Syslog. You have the flexibility to design an alert mechanism based on your requirements.

You can select among **My Rules**, **Used Rules**, **Vendor Rules**, **Shared Rules**, and **Transferred Rules** from the drop-down at the top-left corner of the panel.

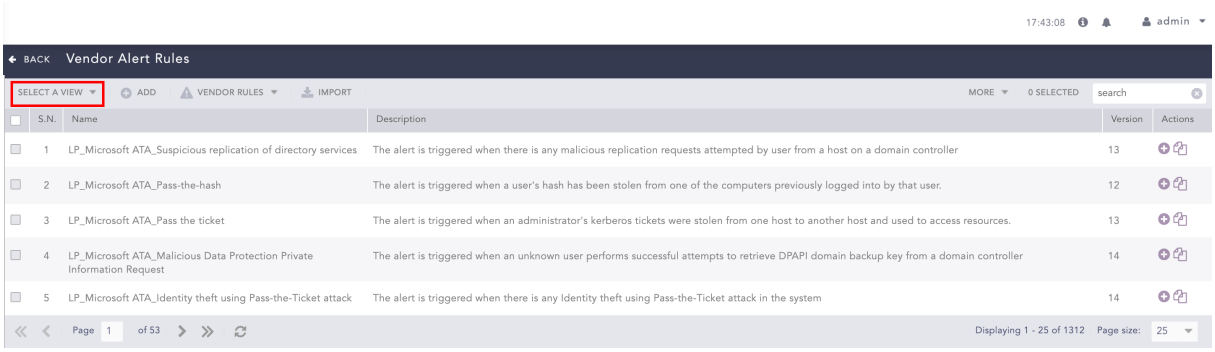
NOTE
If you use a log_ts timestamp to configure the system, SLS does not incorporate older logs in the alerts. So, it does not generate any alerts if there is a delay in the collection time of the logs.

Selecting Page View of Alert Rules

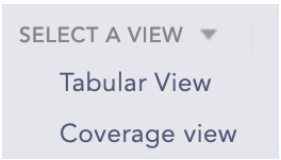
You can view the alert rules in two ways:

- Tabular view
- Coverage view

1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.



2. Select the required view from the **Select a view** drop-down.

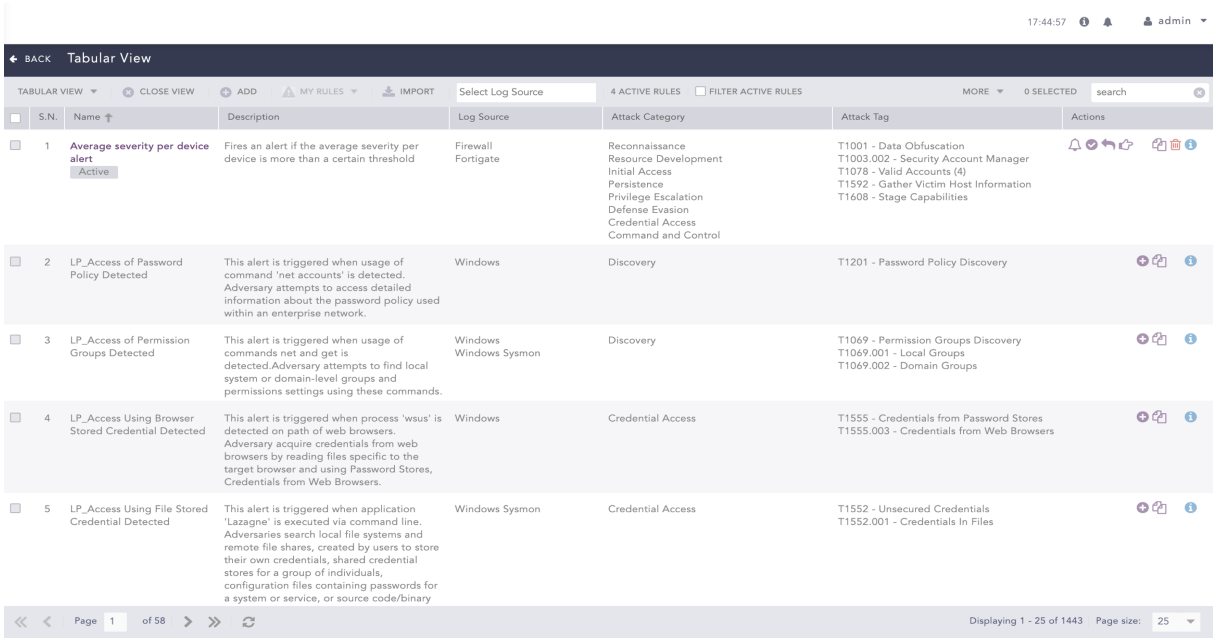


NOTE
Only the alert rules under **My Rules**, **Used Rules**, **Vendor Rules** and used **Shared Rules** can be viewed from the views.

Tabular View

You can select the **Tabular view** option to display additional columns listing the **Log Source**, **Attack Category**, and **Attack Tag** associated with the alert rules on top of the default alert view.

The **Name** column also features a tag to indicate the active/inactive status of the alert rule.



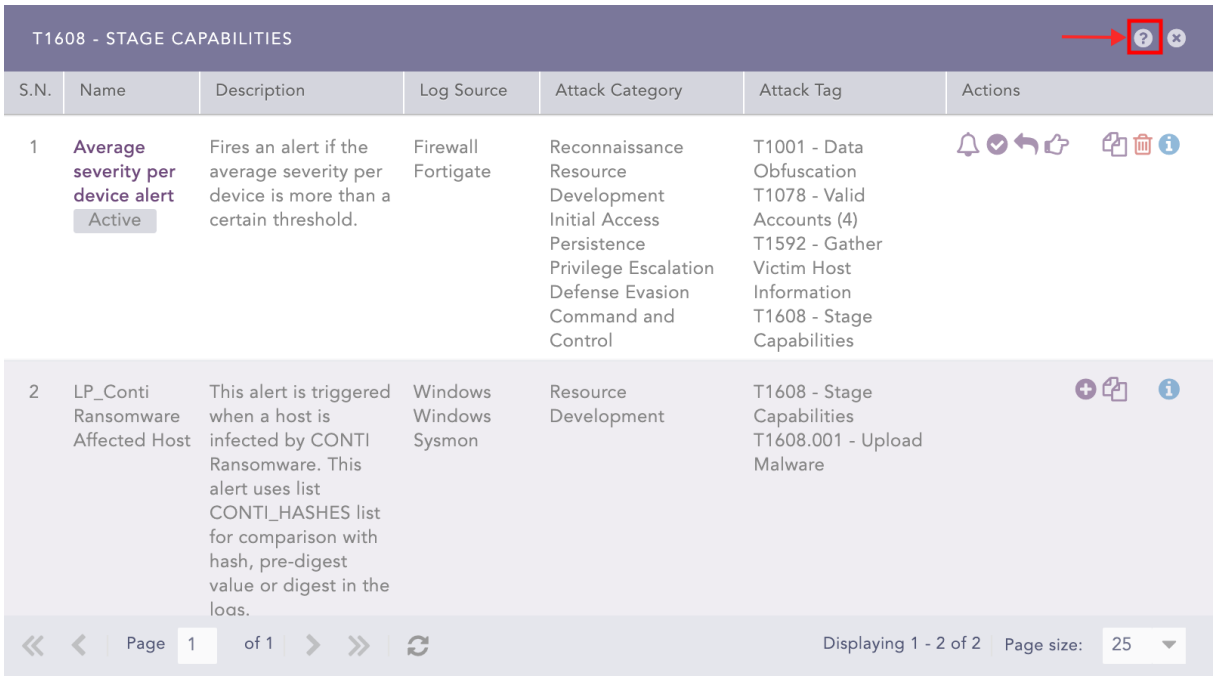
Coverage View

You can select the **Coverage view** option to view the categorization of the alert rules based on various attack categories and attack tags associated with the attack tactics, attack techniques and, attack sub-techniques of the MITRE attack framework. The attack categories are displayed as column headers with the respective attack tags listed under. You can further drill down the attack tags.

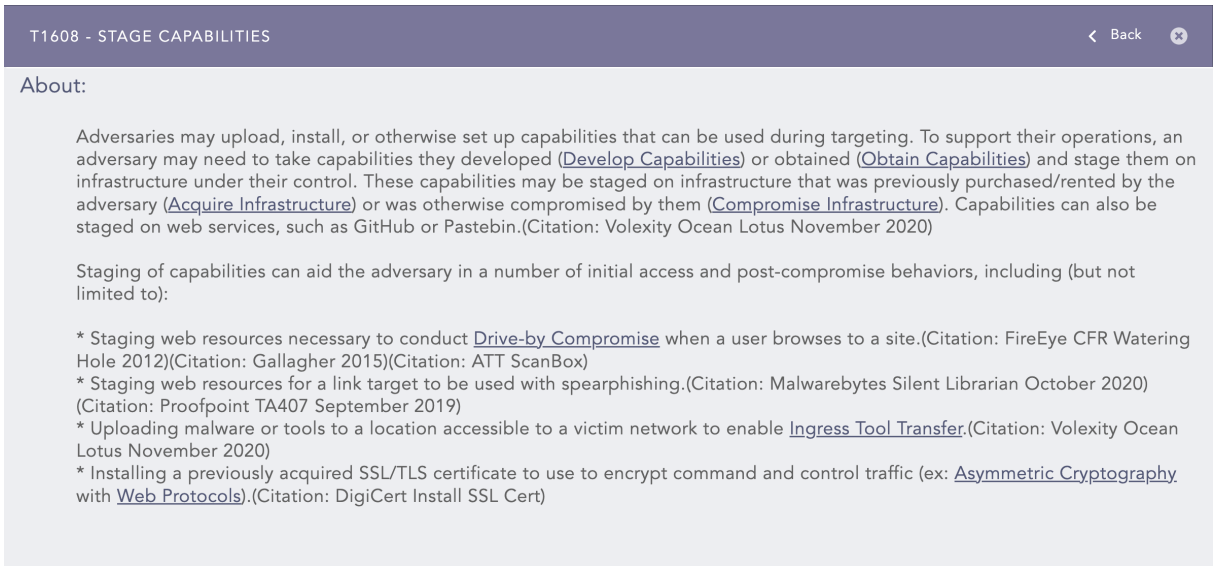
You can click the attack tags to view the list of associated alerts rules. The alert rules are listed as similar to the tabular view.

NOTE

- The total count of active alerts rules with respect to the total number of alert rules is highlighted in green under the attack tag.
- The total count of alert rules doesn't change when the vendor alert rules are used; however, the used vendor alerts are listed along with the vendor alert rule in the dialog box.



Click the help ( ) icon on the top of the dialog box to view the description of the attack tag associated with the attack techniques and sub-techniques of the MITRE attack framework.



View Actions

The tabular/coverage view consists of an action bar allowing you to perform the following actions:

Add

Allows you to create a new alert rule using the alert creation wizard. Refer to Creating an Alert Rule for more details.

Import

Allows you to import alert rules from the stored location. Refer to Importing Alert Rules for more details.

Close view

Allows you to close the tabular/coverage view and return to the **My Alert Rules** page.

Filter Active Rules

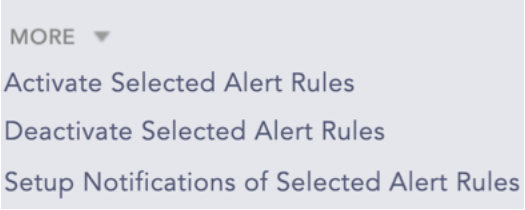
Allows you to view only the active alert rules by selecting the checkbox. This checkbox is only available for tabular view.

Select Log Source

Allows you to filter the alert rules according to the log sources using the drop-down. The drop-down is only available for tabular view.

More

The More drop-down near the top-right corner of the tabular view page lists additional actions.

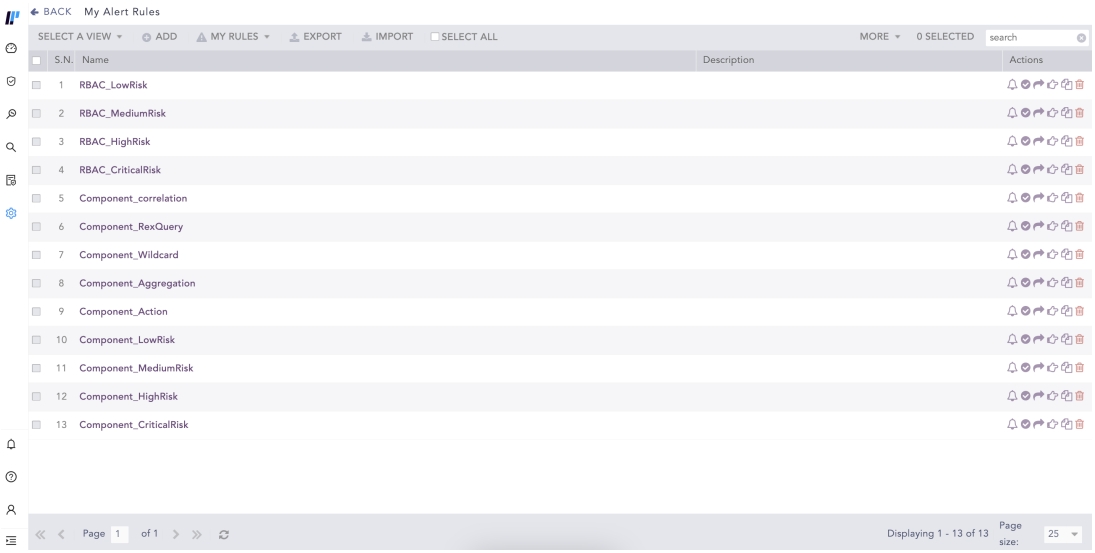


- The **Activate Selected Alert Rules** option lets you activate multiple alert rules at once.
- The **Deactivate Selected Alert Rules** option lets you deactivate multiple alert rules at once.
- The **Setup Notifications of Selected Alert Rules** option lets you configure alert notification for multiple alerts at once. Refer to Setting Up Alert Notifications for more details.

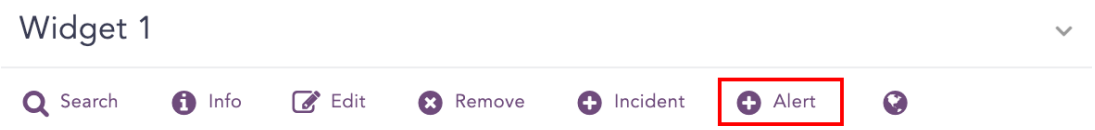
Creating an Alert Rule

Alert rules can be based on any SLS query to check logs for signs of malicious activity, or for certain operational messages and thresholds.

1. There are two ways to create an alert rule.
   - Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**, then click **ADD**.



   - From a dashboard or search template widget, at the top right click **Alert**. If you are creating an alert rule from a widget, SLS automatically adds the widget's query in the Query field.



2. You are taken to the Create New Alert Page. You can also go to **Overview** and click on **Edit** to move to the specific field.

Create New Alert

Overview | Parameters | Criteria | Meta-Data | Ownership | Data Template

Name: Edit
None

Description: Edit
None

Query: Edit
None

Alert Rule ID:
None

Parameters:

Field	Value	
Repos	None	Edit
Query Time-range	None	Edit
Search Interval	None	Edit
Delay Alert	None	Edit
Flush on Trigger	False	Edit
Alert Throttling	None	Edit

Criteria:

Field	Value

Cancel | Create Alert

Create New Alert

Overview | Parameters | Criteria 1 | Meta-Data | Ownership | Data Template

* Name

Average Severity per device

Description

Average Severity per device

* Query

severity=*|chart avg(severity) by device_ip

Browse

* Repos

_LogPointAlerts x _logpoint x new_Repo x

* Query Time-range

10 Minutes

Results Limit

25

Data Privacy Module: Alert Using Original data

Data Privacy Module is enabled in this machine. By Default the alert will be generated with encrypted data. If you want the generate the alert with original data, you will need permission.

Search Interval

5 (Default) Minutes

Set Search Interval to specify the time for Logpoint to perform the next search. The interval should be a factor of the query time range.

Delay Alert

1 Minutes

Set Delay Threshold to specify the wait time for the Alert. Alert is triggered only after the configured time, including late-arriving logs.

Flush On Trigger

Once an alert is triggered, the next alert will be triggered only by a new set of events

Alert Throttling

Field

Time

0 Minutes

Once an alert is triggered, another alert will not be triggered for the same set of values of the selected field until the specified time

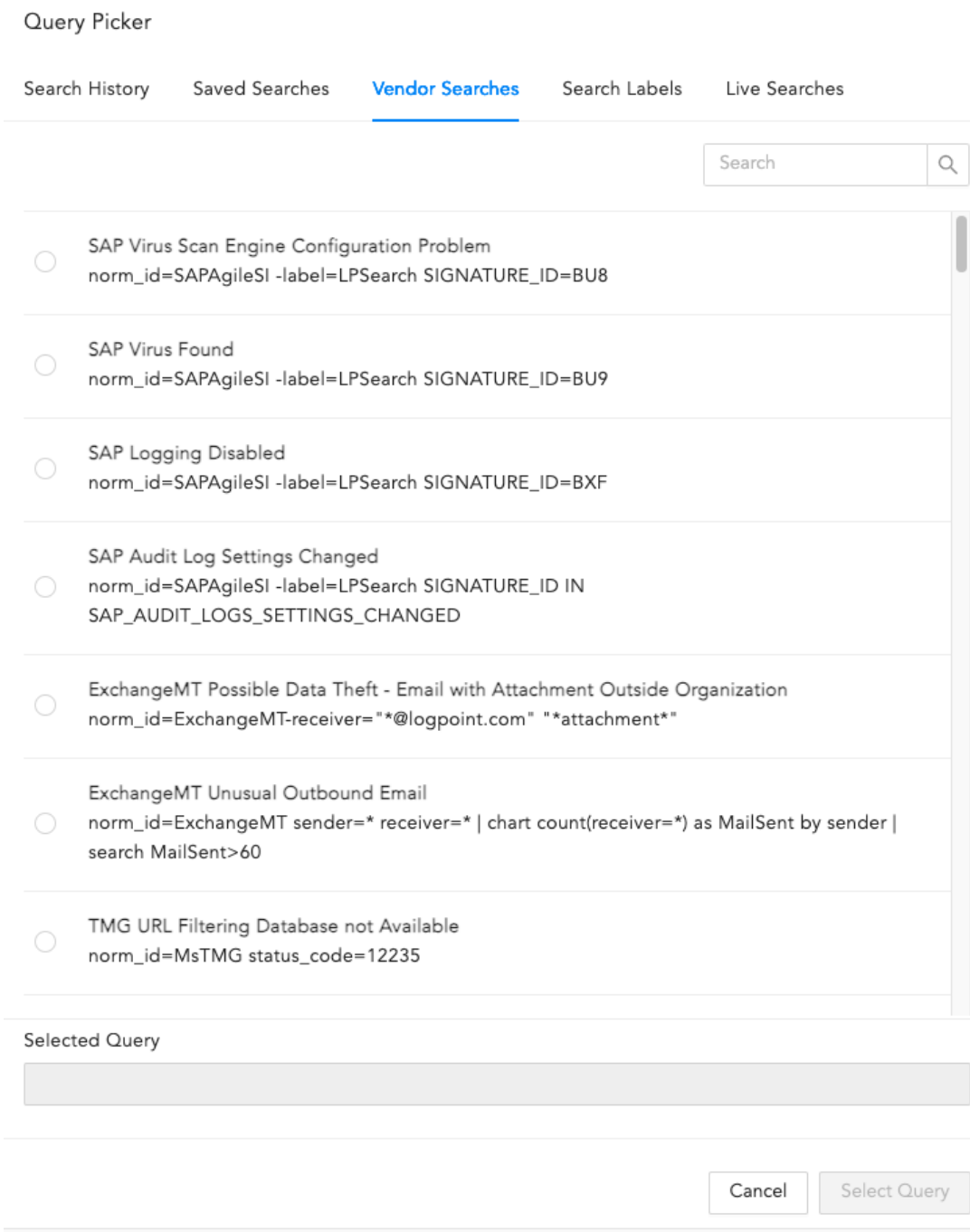
Cancel Create Alert

3. Enter the **Name** of the alert.
4. Enter a **Description**.
5. In **Query**, enter an alert query manually or click **Browse** to select one using the Query Picker.

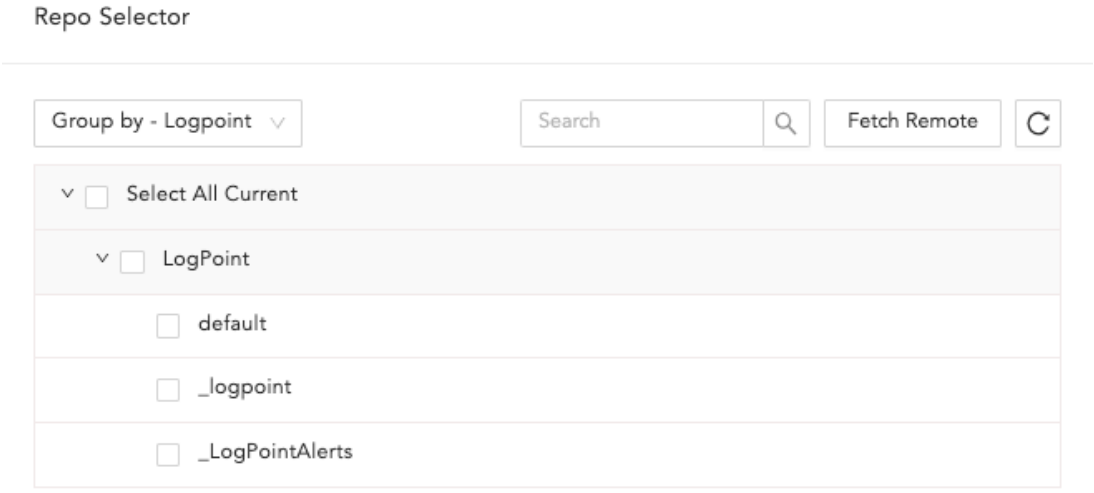
> **NOTE**
> If the **Data Privacy** is enabled, the values for all the configured Data Privacy Module fields are encrypted. For queries that have specific configured fields values, SLS does not generate an incident. However, for the queries that have all their values an incident is generated with encrypted field values.
> For example, if you have configured the **device_name** field under the **Data Privacy Module**, then the query **device_name=localhost** does not generate any incident. However, the query **device_name=*** generates the incidents with encrypted values.

If you use the Query Picker, you can base the query on:

- **Search History**: All the search history of your SLS.
- **Saved searches**: Saved SLS searches.
- **Vendor searches**: Vendor-provided searches.
- **Search Labels**: Search labels.
- **Live Searches**: Queries used by other created alerts.


Query Picker
Search History
Saved Searches
Vendor Searches
Search Labels
Live Searches
Search
SAP Virus Scan Engine Configuration Problem
norm_id=SAPAgileSI -label=LPSearch SIGNATURE_ID=BU8
SAP Virus Found
norm_id=SAPAgileSI -label=LPSearch SIGNATURE_ID=BU9
SAP Logging Disabled
norm_id=SAPAgileSI -label=LPSearch SIGNATURE_ID=BXF
SAP Audit Log Settings Changed
norm_id=SAPAgileSI -label=LPSearch SIGNATURE_ID IN SAP_AUDIT_LOGS_SETTINGS_CHANGED
ExchangeMT Possible Data Theft - Email with Attachment Outside Organization
norm_id=ExchangeMT-receiver="*@logpoint.com" "*attachment*"
ExchangeMT Unusual Outbound Email
norm_id=ExchangeMT sender=* receiver=* | chart count(receiver=*) as MailSent by sender | search MailSent>60
TMG URL Filtering Database not Available
norm_id=MsTMG status_code=12235
Selected Query
Cancel
Select Query

6. Select the **Repos** to be monitored to match the alert condition. You can also select the repo using **Repo Selector** by clicking on **Advanced Selection**.

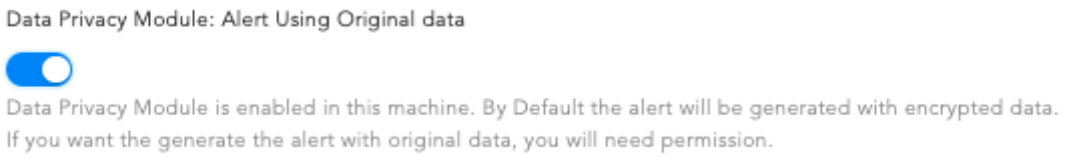


In **Repo Selector**, you can fetch all the repos from remote SLSs by clicking **Fetch Remote**.

7. Select a **Query Time-range** for the alert. Query Time-range is a time frame within which the search is performed. For example, when the query time range is set to 3 days, the system will search for logs from last 3 days.
You can set a time range in either minutes, hours or days. The maximum time range limit is 30 days or its equivalent in hours and minutes.
8. In **Results Limit**, enter the maximum number of logs to retrieve using the Query.

> **NOTE**
> The **Results Limit** field is hidden if you enter an aggregation query in the Query field.

9. If **Data Privacy** is enabled, you will see **Data Privacy Module: Alert Using Original data**. This determines whether the data is encrypted or not. By default they are encrypted. To decrypt them, select **Alert Using Original Data**.



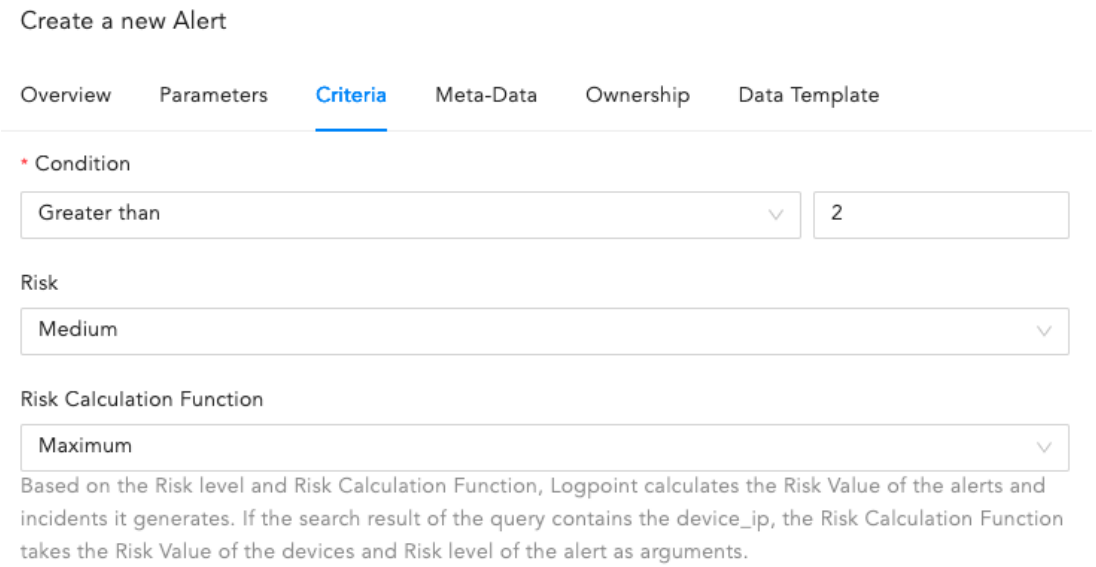
10. Select the **Search Interval**. If you set the search interval to two, SLS performs the search every two minutes.

> **NOTE**
> - The **Search Interval** should be a factor of the **Query Time-range** value in minutes. SLS recommends changing the **Search Interval** of any previously configured alert rules to the factor of the **Query Time-range** value in minutes.
> - Search Intervals do not work with correlation queries. Therefore, if you have used a correlation query in the **Query** field, the search is not performed in the specified **Search Interval**.

11. Enter the **Delay Alert**. SLS waits until the delay time passes before processing the logs to ensure that all relevant logs are collected before generating any incidents.

> **IMPORTANT**
> - **Delay Alert** can only be used with **log_ts** based searches.
> - While defining **Search Interval** and **Delay Alert**, we recommend you define the delay alert value in the multiple of the search interval value. For example: If the search interval is 5 min, the recommended delay alert is 5 min, 10 min, 15 min, 20 min and so on.
> - The maximum value of the **Delay Alert** can be up to 24 hours.

12. Enable **Flush On Trigger** if you want the next alert triggered only based on a new set of events.
13. Set **Alert Throttling** to ensure that SLS does not create multiple alerts for the same set of values for a specified time. Provide the **Field** and the time in **Minutes**. Once an alert is triggered for a value set of the particular **Field**, it does not trigger another alert with the same set of values until the time specified Minutes.
14. Go to **Criteria**.



15. Select the **Condition**, **Risk**, and **Risk Calculating Function** from the drop-downs.

    Based on the **Risk** level and **Risk Calculation Function**, SLS calculates the **Risk Value** of the alerts and incidents they generated. If the search result of the query contains the [device_ip], the **Risk Calculation Function** takes the **Risk Value** of the devices and **Risk level** of the alert as arguments.

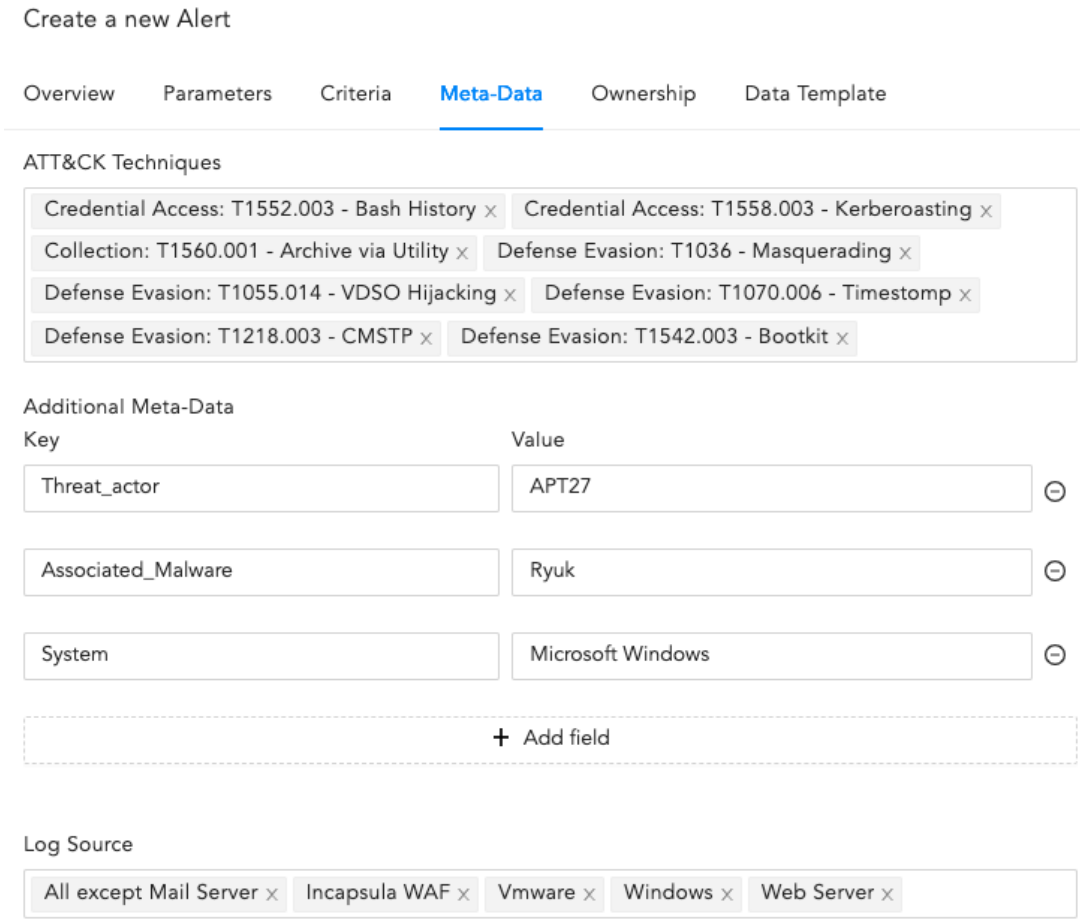
    For example:
    If the **Risk** level of an alert is **Medium**, **Risk Calculation Function** is **Maximum**, and the **Risk Value** of its associated device(s) is **Critical**, the **Risk Value** of the generated alert and incident is: [Maximum(Risk level, Risk value of device(s))]. That means the Risk value of the incident is Critical.
    The risk value of a device is calculated from the values of Confidentiality, Availability, and Integrity.

    Whereas for search queries with pipeline commands or without [device_ip] in the search results, the **Risk Value** of the alert and its generated incident(s) is equal to the **Risk** level of the alert.

    Condition is the number of logs the search will return. Setting a limit controls the number of logs for the search. The number of logs you select should not exceed the previously set limit. SLS compares the limit value to the value set in the condition to the added alert rule. For example, you set the limit to 30 logs. Then you need to make sure that your condition is 30 or less. It cannot be greater than 30.

    Average returns the average of the sum of **Confidentiality**, **Availability**, **Integrity**, and **Risk** divided by the number of times they happened. **Maximum** returns the highest value and **Minimum** returns the lowest.

16. Go to **Meta-Data**.

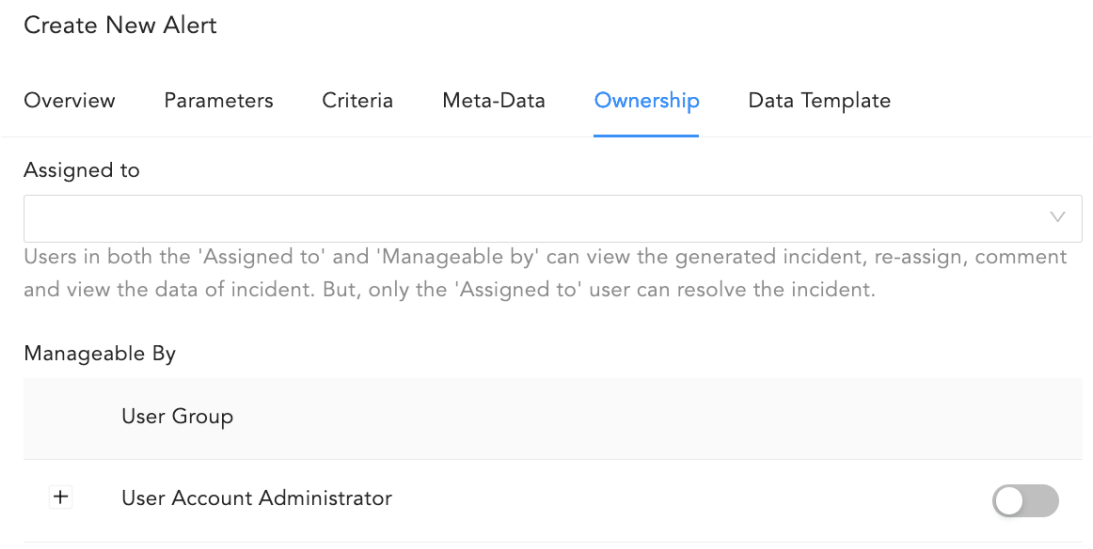


17. Select the **ATT&CK Techniques** from the drop-down. You can select multiple techniques to categorize the alert.
18. Provide **Additional Meta-Data** as **Field** and **Value** to categorize the alert rules. You can add new fields and values by clicking **Add Field**. The Metadata Field should contain letters or a combination of letters, numbers, or underscores (_), and must start with a letter.

> **IMPORTANT**
> - You cannot provide SLS reserved Jinja placeholders as Metadata field in the **Field** column.
> - You cannot repeat the Metadata Field.
> - Value associated with the Metadata Field cannot be empty and vice-versa.

19. Select **Log Source** from the drop-down or add new log sources associated with the alert rule.

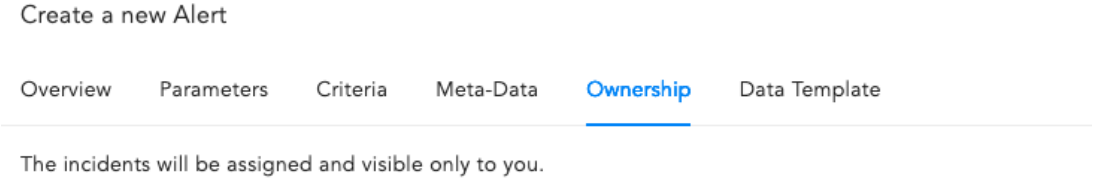
20. Go to **Ownership**.



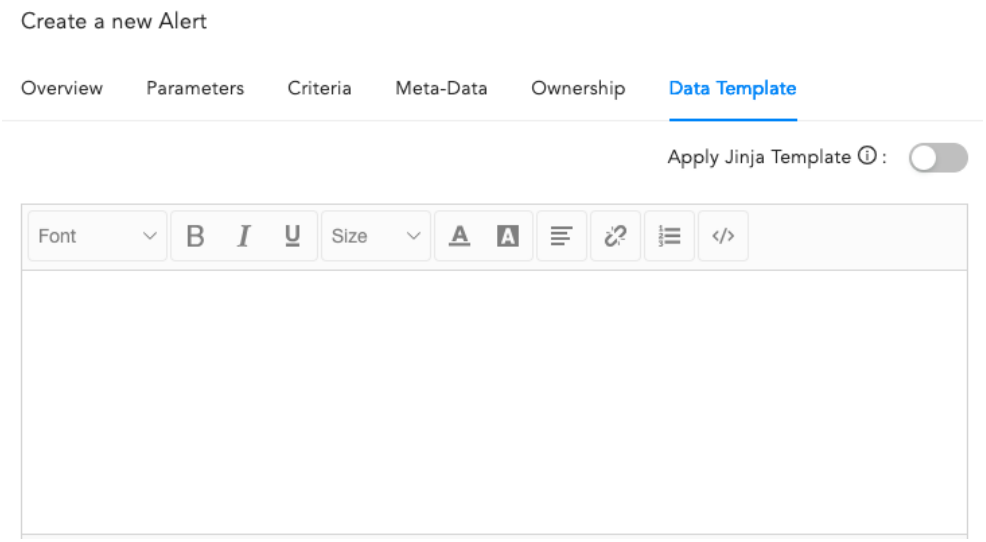
If **Data Privacy Module** is enabled, users with the **Can Grant Access** permission can grant access to alerts to users with the **Can Request Access** permission. If you are a user who can grant access, you can view the requests by going to `Settings >> Configurations >> Data Privacy Module >> Pending Request`.
If you are a user who requested access to an alert, you can view the status of your requests by going to `Settings >> Configurations >> Data Privacy Module >> My Request`.

21. You need to assign the Alert rule to a user, user group or yourself. Assigned users can re-assign, comment on, and view the data of the generated incident. They can also resolve the alert.
Alert Rules can be exported and imported. If you export an Alert Rule, ownership is lost. If you import an Alert Rule, you get ownership or the person who performs the import will.
To assign the alert to :
    - An individual user, use the **Assigned to** drop-down to select them.
    - A group, use the **Manageable By** to select them.
    - To yourself, deselect all of the Incident User Groups in **Manageable By**.

    If you do not belong to any **Incident User Groups**, both the Assigned to and Manageable by are hidden and in SLS you get the following:

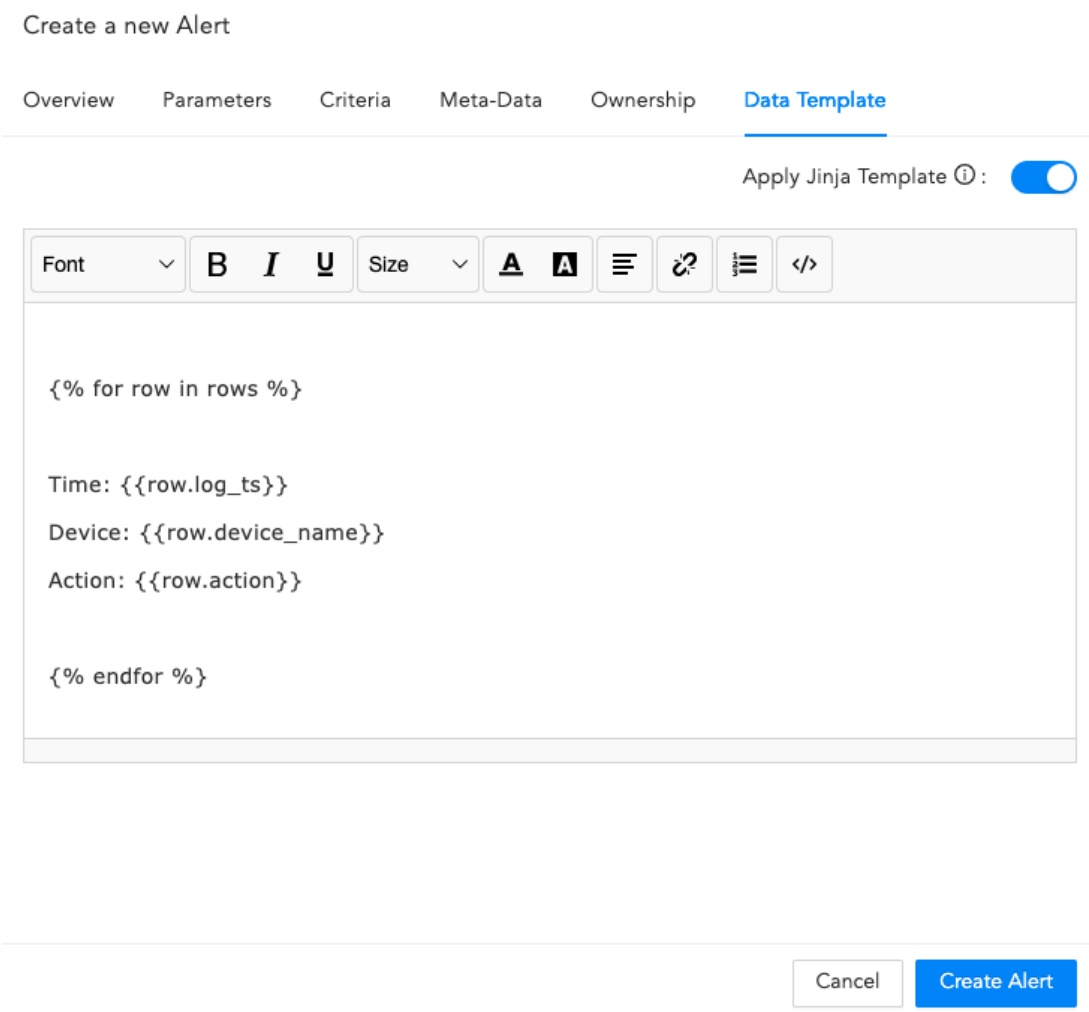


22. Go to **Data Template**.

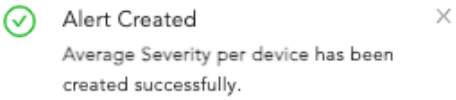


23. Enable **Apply Jinja Template** and enter the template in the text field. SLS allows you to view the details of the incidents triggering the alert in a format specified in a Jinja template.

> **IMPORTANT**
> If the Jinja template has a timestamp, the **datetime** filter is mandatory when you want the date clearly displayed. The timestamp will be in raw epoch format if the filter is not included.



24. Click **Create Alert**.
When the alert is successfully created, you will get a confirmation message.



After configuring the Alert Rule, SLS automatically notifies you when an alert is triggered. Go to Setting Up Alert Notifications to learn how to set up alert notifications.

An alert is triggered and an incident for the alert is generated every time the search query meets all the alerting criteria.

To view all incidents, go to the Navigation bar and click **Incidents**.

Setting Up Alert Notifications

To set up alert notifications, click the **Setup Notification** ( ) icon of the corresponding alert rule. The **Setup Notifications** dialog box provides you with multiple options to configure the alert notification.

NOTE

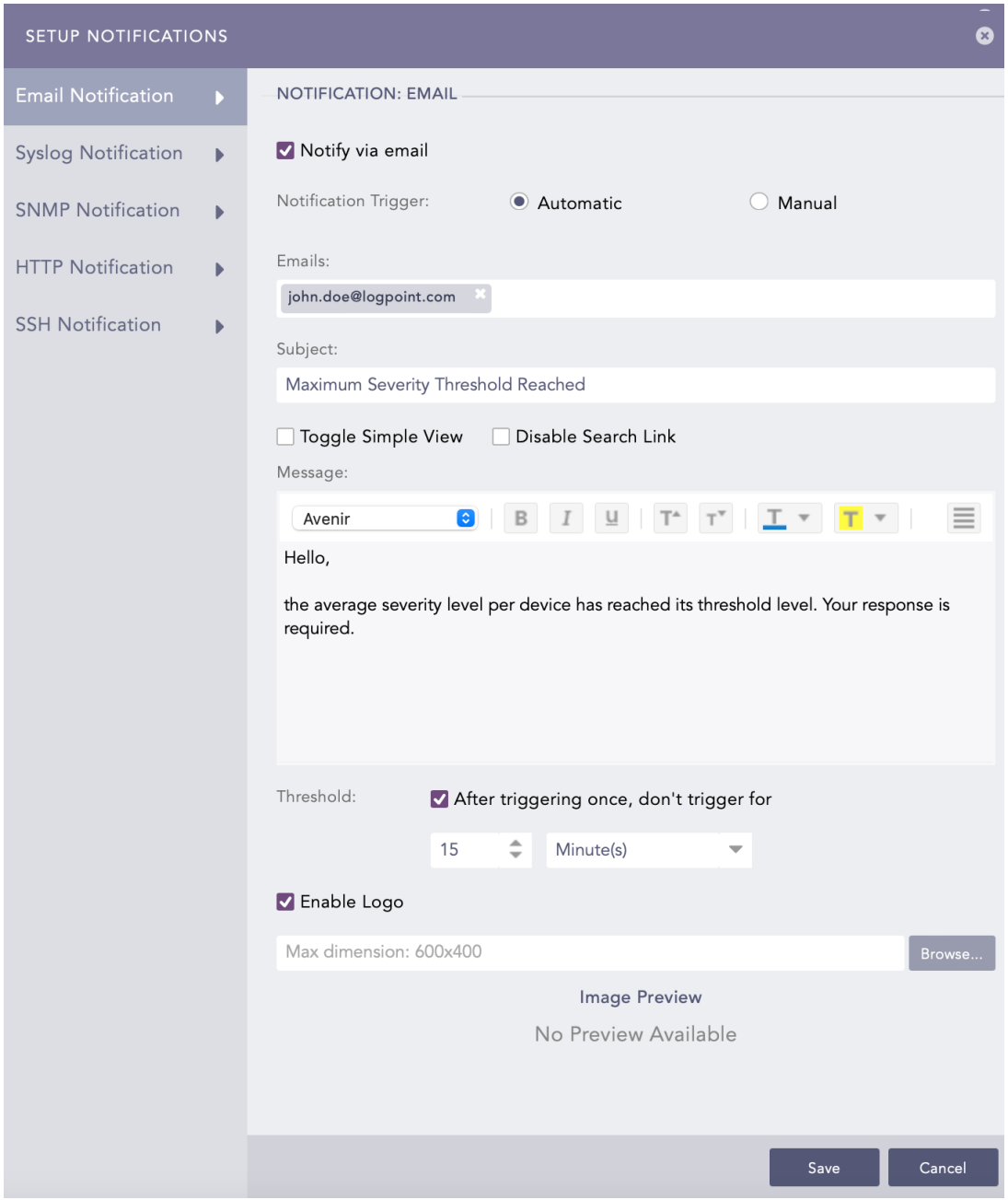
The solid bell icon () under the **Actions** column indicates notification-enabled alert rules, while the outline bell icon () indicates notification-disabled alert rules.

Configuring Email Notification

NOTE

You must configure the **SMTP** service before sending email notifications.

1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Click the **Setup Notification** () icon from the **Actions** column of the alert rule.
3. Click **Email Notification** and select **Notify via email**.



4. In **Notification Trigger**:
   - Select **Automatic** to send a notification every time the alert rule is triggered.
   - Select **Manual** to manually send the notification from the Incident Actions.
5. Enter valid email addresses in **Emails**.

6. Enter a **Subject**. SLS supports various Jinja commands for alert rules such as: `{{alert_name}}`, `{{detection_timestamp}}`, `{{risk_level}}`, `{{rows}}` and `{{rows_count}}`. You can write them in the **Subject** field as:

```
Logs from {{rows[0].col_type}} on date {{rows[0].col_ts|datetime}}
```

You can use the Jinja commands `{{attack_id}}`, `{{attack_tag}}`, `{{attack_category}}`, and `{{log_source}}` in the **Subject** and **Message** fields. You can also use the Jinja commands in the alert's metadata fields. You can use the metadata fields **threatactor**, **Associated_Malware**, and **System**, as Jinja commands `{{threatactor}}`, `{{Associated_Malware}}`, and `{{System}}`.

Some example Jinja commands that you can use in email subject and message fields are:

Jinja template to display devices that sent logs:

```
{% for row in rows %}
Device: {{row.device_name}}
{% endfor %}
```

Jinja template to display severity-based message:

```
{% if risk_level == "medium"%}

    <p style="color:yellow"> You need not take any action </p>

{% elif risk_level == "high"%}

    <p style="color:red"> Take action immediately </p>

{% endif %}
```

To learn more about which Jinja commands you can use for the **Subject** and **Message** fields, go to SLS Reserved Jinja Placeholder.

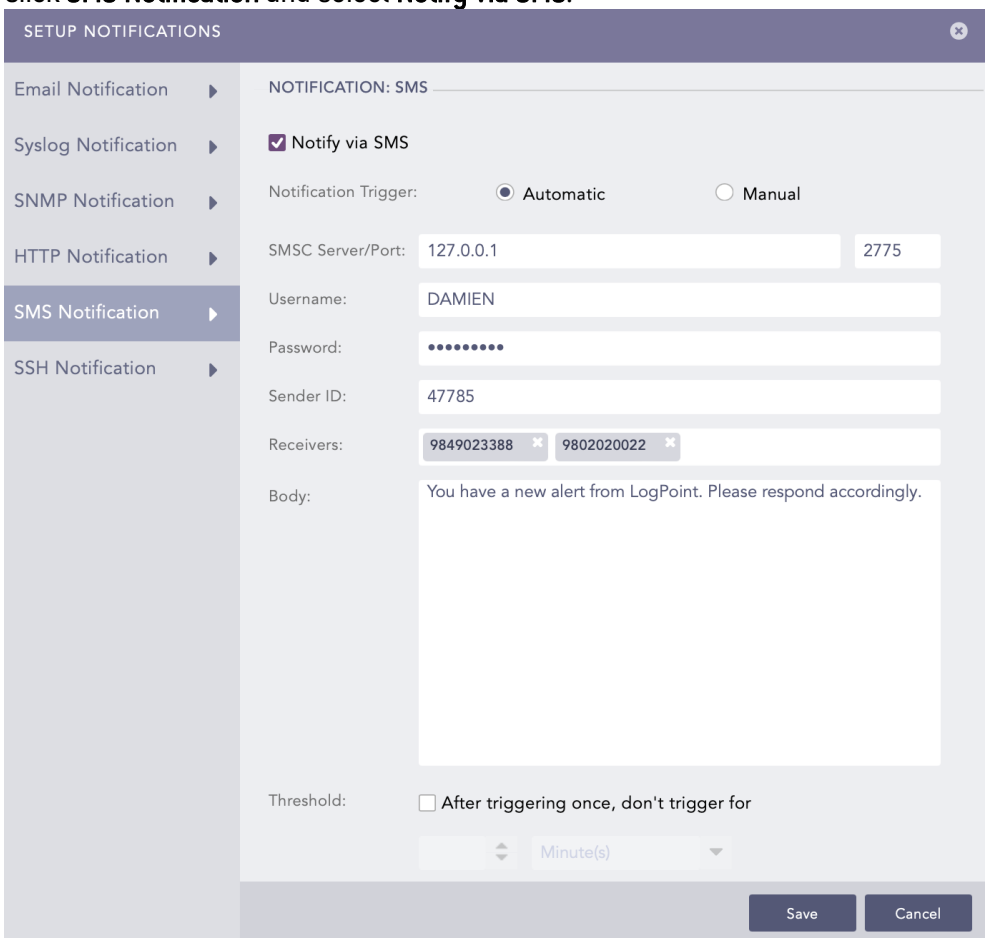
7. Select **Toggle Simple View** to enable or disable the advanced text editor.
8. Select **Disable Search Link** to remove the search link in the email. The search link redirects to the search page of the SLS machine from which the email notification is configured.
9. Enter a **Message**.
10. Set the **Threshold**.
11. Select **Enable Logo** if you want to include the SLS logo in the email notification. If you do not want to include the SLS logo in the email, deselect **Enable Logo** and click **Save**.
12. **Browse** for the image in the JPG/JPEG format if you want to provide a custom logo. The maximum dimension for the custom logo is 600*400.
13. Click **Save**.

Configuring SMS Notification

Before configuring SMS notification, SMSC server must be accessible from SLS.

1. Go to `Settings >> Knowledge Base` and click **Alert Rules**.
2. Click the **Setup Notification** ( ) icon from the **Actions** column of an alert rule.

3. Click **SMS Notification** and select **Notify via SMS**.



4. In **Notification Trigger**:
   - Select **Automatic** to send an sms notification every time the alert rule is triggered.
   - Select **Manual** to manually send the sms notification from the Incident Actions.
5. Enter **SMSC Server/Port**. The SMSC server supports both hostname and IP address.
6. Enter **Username**, **Password**, and **Sender ID** of the server.
7. In **Receivers**, enter the phone numbers of the receivers. You can also include country code if necessary.
8. In **Body**, enter the SMS message. You can also use Jinja commands. We recommend you use a placeholder of Jinja commands like `{{alert_name}}`, `{{detection_timestamp}}`, `{{risk_level}}`, `{{rows}}` and `{{rows_count}}` in **Body**. You can also use the Jinja commands in the alert's metadata fields. You can use the metadata fields **threatactor**, **Associated_Malware**, and **System**, as Jinja commands `{{threatactor}}`, `{{Associated_Malware}}`, and `{{System}}`.

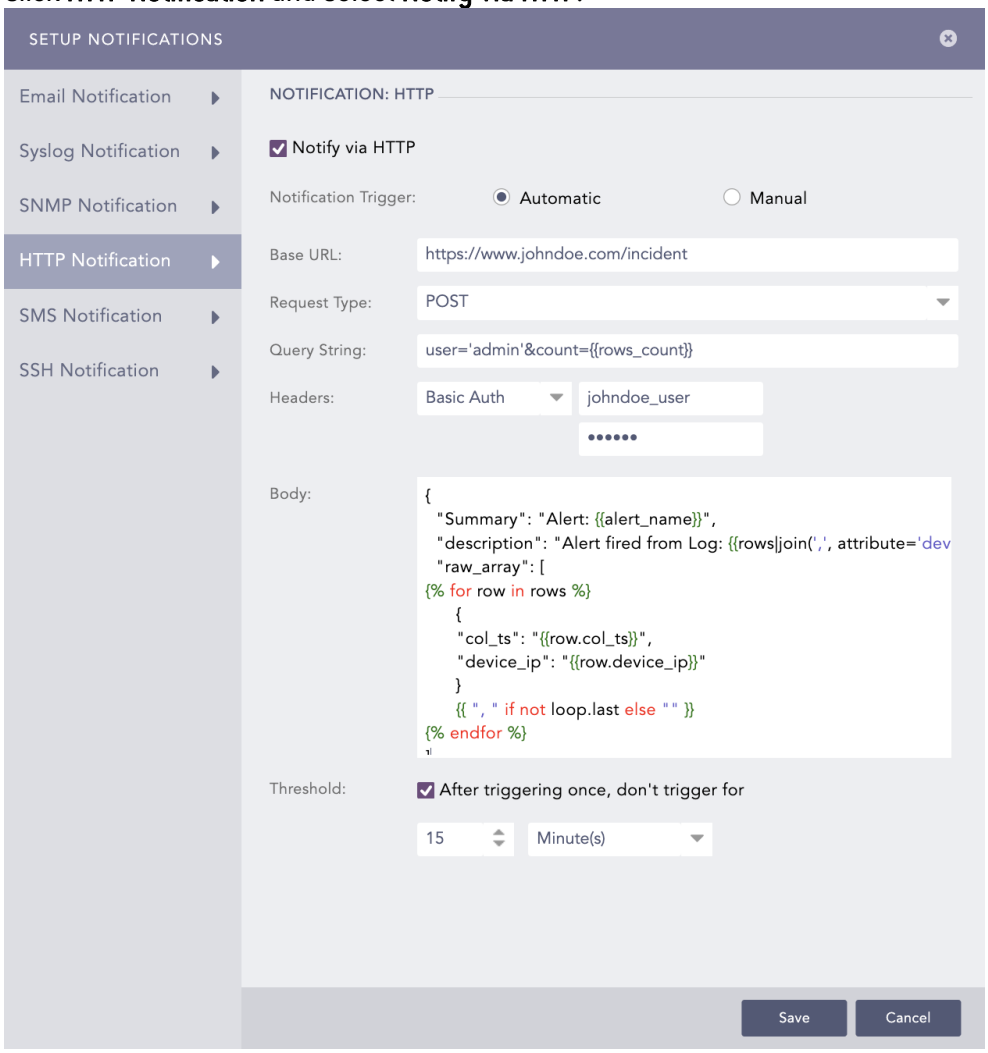
   Jinja template to display timezone of devices that sent logs:

   ```
   {% for row in rows %}
   Time Zone: {{row.timezone}}
   {% endfor %}
   ```

   To learn more about Jinja commands, go to SLS Reserved Jinja Placeholder.
9. Set the **Threshold** time to trigger the SMS notification after enabling it.
10. Click **Save**.

Configuring HTTP Notification

1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Click the **Setup Notification** ( ) icon from the **Actions** column for the alert rule.
3. Click **HTTP Notification** and select **Notify via HTTP**.



4. Under **Notification Trigger**:
   - Select **Automatic** to send a notification every time the alert rule is triggered.
   - Select **Manual** to manually send the notification from the Incident Actions.
5. Provide either a valid IP address or domain name in the **Base URL** field.
6. Select a **Request Type** from the drop-down.

7. Provide a **Query String**. SLS supports various Jinja commands for alert rules. They are `{{alert_name}}`, `{{detection_timestamp}}`, `{{risk_level}}`, `{{rows}}`, and `{{rows_count}}`. You can write them in query as:

```
user='admin'&count={{rows_count}}
```

You can use the Jinja commands `{{attack_id}}`, `{{attack_tag}}`, `{{attack_category}}`, and `{{log_source}}` in the **Query String** and **Body** fields. You need to input JSON string in the **Body** field. You can also use the Jinja commands in the alert's metadata fields. You can use the metadata fields **threatactor**, **Associated_Malware**, and **System**, as Jinja commands `{{threatactor}}`, `{{Associated_Malware}}`, and `{{System}}`.

Jinja template to display list of alerts and associated device ips:

```
{

    "Summary": "Alert: {{alert_name}}",

    "description": "Alert fired from Log: {{rows|join(',',
attribute='device_ip')}}",

    "raw_array": [

{% for row in rows %}

        {

        "col_ts": "{{row.col_ts}}",

        "device_ip": "{{row.device_ip}}"

        }

        {{ ", " if not loop.last else "" }}

{% endfor %}

]

}
```

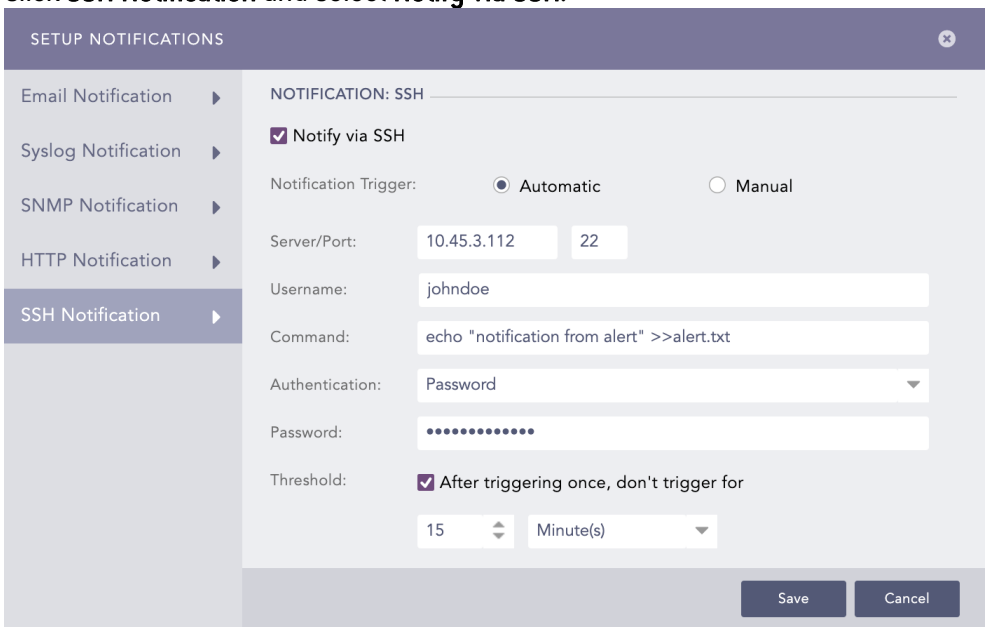
To learn more about which Jinja commands you can use for the **Query String** and **Body** fields, go to SLS Reserved Jinja Placeholder.

8. Select an authentication **Header** type.
   - If you select **Basic Auth**, enter the **Key** and **Password**.
   - If you select **API Token**, enter the **Key** and **Value**.
   - If you select **Bearer Token**, enter the **Key**.
9. Enter a template for the **Body** of the HTTP notification in Jinja format.
   You can enter the template only for the **POST**, **PUT**, and **PATCH** request methods.
10. Set the **Threshold**.
11. Click **Finish**.

SMTP and SSH services can have Jinja2 Syntax as message or command.

Configuring SSH Notification

1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Click the **Setup Notification** ( ) icon from the **Actions** column of the alert rule.
3. Click **SSH Notification** and select **Notify via SSH**.



4. In **Notification Trigger**:
   - Select **Automatic** to send a notification every time the alert rule is triggered.
   - Select **Manual** to manually send the notification from the Incident Actions.
5. Enter a **Server** address and a **Port** number.
6. Enter a **Username** for the user in the destination server.
7. Enter a **Command** you want to execute when the alert rule is fired. Make sure that the command is a valid bash command and is executable.
   You can use the Jinja commands `{{attack_id}}`, `{{attack_tag}}`, `{{attack_category}}`, and `{{log_source}}` in the **Command** field. You can also use the Jinja commands in the alert's metadata fields. You can use the metadata fields **threatactor**, **Associated_Malware**, and **System**, as Jinja commands `{{threatactor}}`, `{{Associated_Malware}}`, and `{{System}}`.

   Jinja template to write list of log datetime on a file:

```
echo -e "{% for row in rows %}{{row.log_ts|datetime('%B %d')}}{%
endfor %}" >> /home/johndoe/file.txt
```

> **NOTE**
> This command writes a list of log associated datetime on **file.txt** which is located inside /home/johndoe/.

   To learn more about which Jinja commands you can use for the **Command** field, go to SLS Reserved Jinja Placeholder.

8. Select the required mode of **Authentication**: Password or SSH Certificate.
    1. If you select **Password**, enter a passkey in the **Password** tab.
    2. If you select **SSH Certificate**, select the **Certificate type**: System Certificate or User Certificate. The **SSH Certificate** key is automatically generated. You must add the key to the authorized keys at ~/.ssh/authorized_keys in your system.
        - If you select **System Certificate**, SLS uses system-specific certificate for authentication.
        - If you select **User Certificate**, SLS uses individual user-specific certificate for authentication.

    It is important for you to remember the password or the SSH certificate key as it is required later for user-validation.
9. Set the **Threshold**.
10. Click **Finish**.

Configuring SNMP Notification

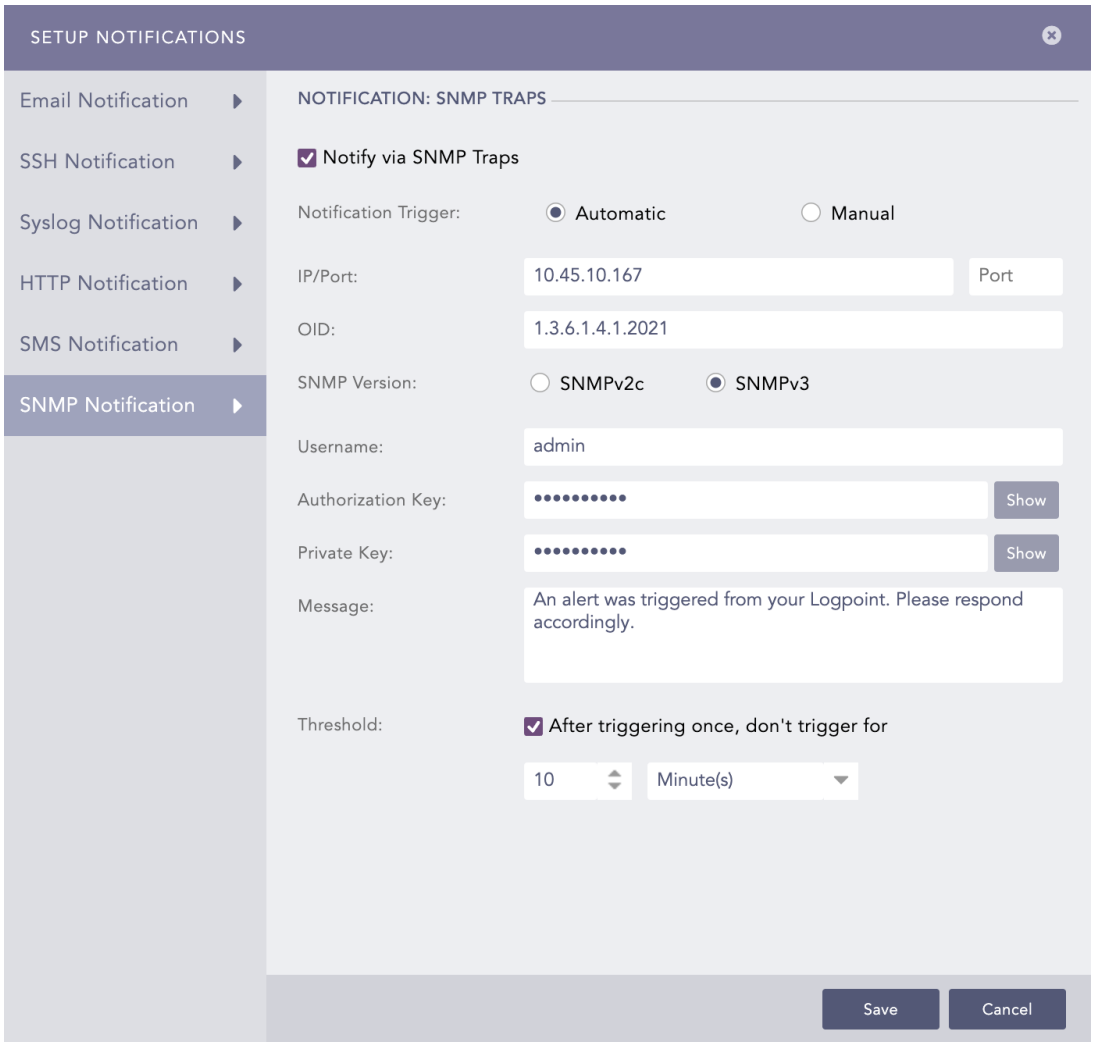
1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Click the **Setup Notification** ( ) icon from the **Actions** column of the alert rule.
3. Click **SNMP Notification** and select **Notify via SNMP Traps**.
4. In **Notification Trigger**:
    - Select **Automatic** to send a notification every time the alert rule is triggered.
    - Select **Manual** to manually send the notification from the Incident Actions.
5. Enter the trap receiver's **IP** address and the **Port** number.
6. Enter a valid SNMP trap or Enterprise specific **OID** (Object Identifier) in the dotted decimal format. Make sure to not use the OID with a leading dot.
7. Select **SNMPv2c** or **SNMPv3** according to the security level you require.
   The notification settings change according to the version you pick.
    - **For SNMPv2c configuration**
        1. Enter the name of the **Agent** that sends the SNMP trap.
        2. Enter a passphrase in the **Community String**. The passphrase should be recognizable by the manager.
        3. Enter the OID's corresponding value in the **Message**.
    - **For SNMPv3c configuration**
        1. Enter the **Username**.
        2. Enter the **Authorization Key** and **Private Key**. You can select whether to **Show** or **Hide** your key.
        3. In the **Message** field, enter the OID's corresponding value.

You can use the Jinja commands like `{{attack_id}}`, `{{attack_tag}}`, `{{attack_category}}`, and `{{log_source}}` in the **Message** field. You can also use the Jinja commands in the alert's metadata fields. You can use the metadata fields **threatactor**, **Associated_Malware**, and **System**, as Jinja commands `{{threatactor}}`, `{{Associated_Malware}}`, and `{{System}}`.

Jinja template to display risk level of alerts:

```
{% for row in rows %}
Risk Level: {{row.risk_level}}
{% endfor %}
```

To learn more about which Jinja commands you can use for the **Message** field, go to SLS Reserved Jinja Placeholder.

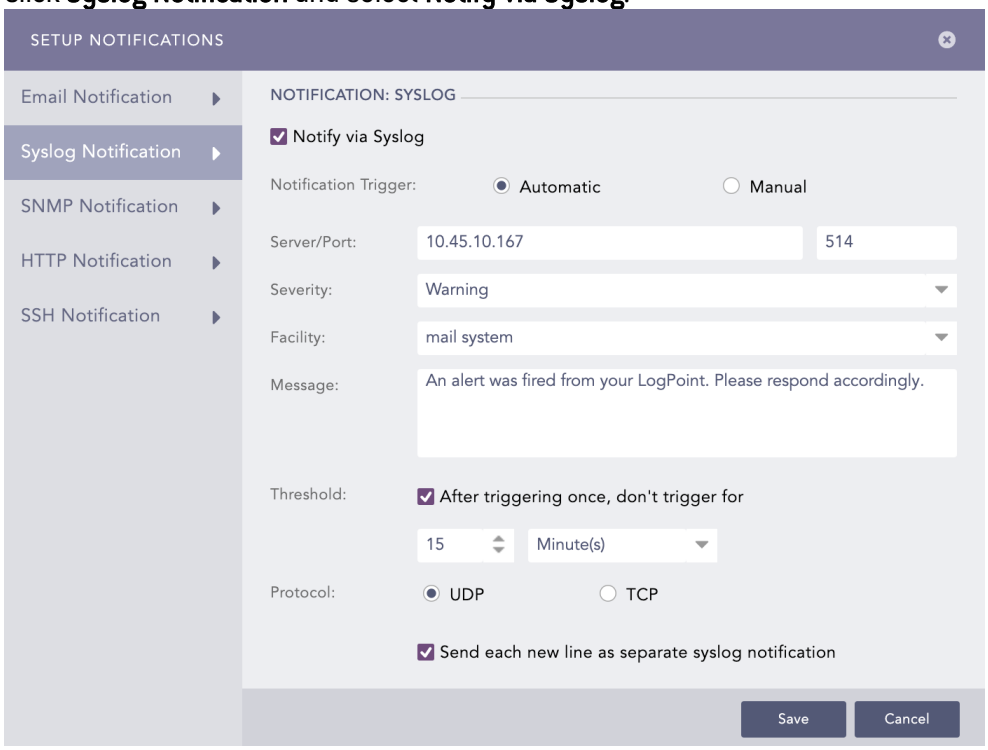


8. Set the **Threshold**.
9. Click **Save**.

Configuring Syslog Notification

1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Click the **Setup Notification** ( ) icon from the **Actions** column of the alert rule.

3. Click **Syslog Notification** and select **Notify via Syslog**.



4. In **Notification Trigger**:
   - Select **Automatic** to send a notification every time the alert rule is triggered.
   - Select **Manual** to manually send the notification from the Incident Actions.
5. Enter the **IP Address** and the **Port** number for the syslog receiver in the **Server/Port** textboxes.
6. Select the level of **Severity** and **Facility** from the drop-downs.
7. Enter a **Message** that provides the information about the event. You can use the Jinja template to construct a message that extracts specific information about the event. You can use the Jinja commands `{{attack_id}}`, `{{attack_tag}}`, `{{attack_category}}`, and `{{log_source}}` in the **Message** fields. You can also use the Jinja commands in the alert's metadata fields. You can use the metadata fields **threatactor**, **Associated_Malware**, and **System**, as Jinja commands `{{threatactor}}`, `{{Associated_Malware}}`, and `{{System}}`.

   Jinja template to send syslog notification with alert name and timestamp

   ```
   {% for row in rows %}
   incident_name: {{alert_name}}; incident_ts: {{row.log_ts}};
   {% endfor %}
   ```

   To learn more about which Jinja commands you can use for the **Message** fields, go to SLS Reserved Jinja Placeholder.
8. Set the **Threshold**.
9. Select the **UDP** or the **TCP** protocol to send the Syslog Notification.
   - If you use UDP, the log message may be dropped or it may arrive out of order.
   - If you use TCP, the log message arrives without being dropped and in order.

10. Select the **Send each new line as separate syslog notification** checkbox to generate one syslog message for each log message in the search results. If you do not select it, all the messages within the chosen time range of the incident are compressed into one syslog message in the search results.
    The **Send each new line as separate syslog notification** option is useful only if the **Message** textbox contains a Jinja template with a **for loop**.

SMTP and **SSH** services can have the **Jinja2** syntax as a message or a command.

For SMTP

For **SMTP**, you can include the **jinja2** syntax in the **Message** textbox to deliver more information about the alert rule fired. Using **jinja2**, you can explain the incident in an elaborate way and can fetch individual data while the alert is fired.

1. **{{rows_count}}** returns the count of the row.
2. **{{rows}}** returns the list of rows returned from search query.

The list returned from **{{rows}}** is in the machine format and difficult to read. For such cases, you can use filter functions along with your jinja syntax. The available filter functions are as follows:

1. **readable**

This command has its effect according to the query provided in alert; for plain search, it returns the result in a list whereas for queries with chart/time chart it displays the output in a tabular form. Use this filter as:

```
{{ rows | readable }}
```

2. **date**

You can convert the fields containing UNIX timestamp in year/month/day format. Use this filter as:

```
{% for row in rows %}
{{row.col_ts | date}}
{% endfor %}
```

3. **time**

This command converts the UNIX timestamp and displays the time in the format hour:minute:second. Use this filter as:

```
{% for row in rows %}
{{row.log_ts | time}}
{% endfor %}
```

4. **datetime**

You can use this syntax to convert datetime from UNIX timestamp. The result is displayed in the year/month/day hour:minute:second format. Use this filter as:

```
{% for row in rows %}
{{row.log_ts | datetime}}
{% endfor %}
```

You can also provide additional parameters to specify the required format.

Syntax to specify the format:

```
datetime (format_string, timezone)
```

For example:

```
{% for row in rows %}
{{row.log_ts | datetime ("%d %m %Y %H:%M:%S", "Asia/Kathmandu")}}
{% endfor %}
```

5. **Iteration Through Values**

You can iterate through the values returned from **{{rows}}**, use loops to view the items returned.

For query

```
error|chart count() by device_ip
```

You can use the following syntax in the message:

```
{%for row in rows%}
{{row.device_ip}}
{%endfor%}
```

This outputs the **device_ip** for every list returned by **rows**.

6. **For Simple Search**

You can use the **readable** function in case of simple search queries. If the parameters returned from the search queries contain UNIX timestamps, then you can use the **date**, **time** or **datetime** to convert them into readable form.

7. **For searches with chart/timechart**

You can use the **readable** function for the clear understanding of the values returned from the **{{rows}}**. If grouping functions used in the search query returns the parameters containing UNIX timestamps, then you can use filter functions **date**, **time**, and **datetime** to convert them into readable form.

NOTE
All the filter functions except the **readable** should be used in loops.

Order of Operations

For query:

```
| chart count(), max(port) as MAX, min(sev,sev>>3) by device_ip, source_
address, step(destination_port,100)
```

You can use the jinja syntax as:

```
{%for row in rows%}
{{row.device_ip}}
{{row.source_address}}
{{row.MAX}}
{%endfor%}
```

NOTE

- The grouping function is written as it is in the query, hence **device_ip** and **source_address** were same in query and syntax.
- Aggregation functions can be mentioned with their aliases; **max(port)** in the search query is denoted as **MAX** in **jinja syntax**.

To minimize confusion, you can use the position of the functions and name them accordingly:

For the query above:

The numbering starts from the first grouping function and goes from left to right as:

```
device_ip= col1
source_address=col2
step(destination_port,100)=col3
```

The complex functions such as **step(destination_port,100)** can not be used directly in **jinja**, the only way to use them is by using displacement count.

Example:

```
{%for row in rows%}
{{row.device_ip}}
{{row.col3}}
{%endfor%}
```

Once the grouping functions are done with naming, the order moves to the beginning of the aggregation function and the numbering goes as:

```
max(field)=col4
min(sev, sev>>3)=col5
```

If aliases are used for aggregation functions, they can be written directly in **jinja syntax**. In the example above, for max(port) the **Jinja** syntax can be written as:

```
{%for row in rows%}
{{row.MAX}}
{%endfor%}
```

NOTE

In case of a timechart, the timechart function itself is treated as an aggregation function as it returns the UNIX-timestamp for the search. In such case, timechart count() is the first aggregation function, and you should name it accordingly. You can use the **jinja syntax** as:

```
{%for row in rows%}
{{row.device_ip}}
{{row.colx}}
{%endfor%}
```

where colx is the displacement count of timechart function.
Timechart can be represented with the **timestamp** so you can write jinja syntax as:

```
{%for row in rows%}
{{row.device_ip}}
{{row.timestamp}}
{%endfor%}
```

For SSH

For **SSH** in the SSH command, you can use the following **jinja2** keywords:

Keyword	Syntax Definition
{{rows_count}}	Number of rows
{{alert_name}}	Name of the alert
{{correlation_name}}	Name of the correlation
{{detection_timestamp}}	Detection timestamp
{{risk_level}}	Risk level

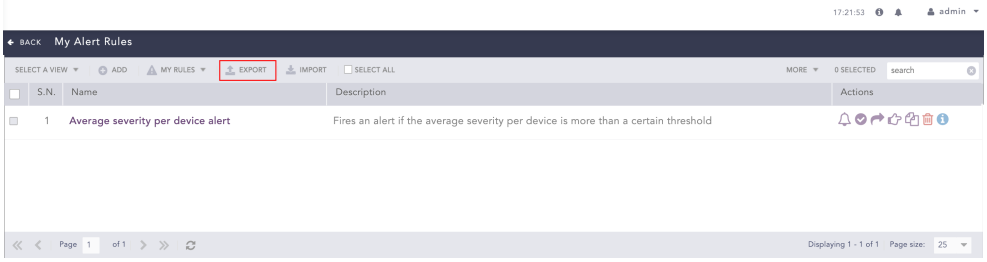
For example:

For the query **User Login**, you can use the command `echo alert with log count = {{rows_count}} with risk_level= {{risk_level}} >> /tmp/login_alert.txt`

After the alert is fired, login_alert text is created at destination location with the number of rows and the risk level of alert.

Exporting Alert Rules

1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.

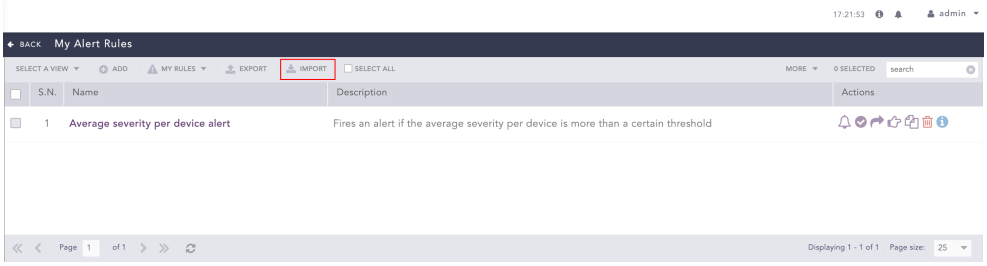


2. Select the alert rules that you want to export.
3. Click **EXPORT**.
   The exported alert rules .pak file also contains the repo configuration of the alert rules.

Importing Alert Rules

While importing alert rules, only the repos from the alert rules exported from SLS are selected.

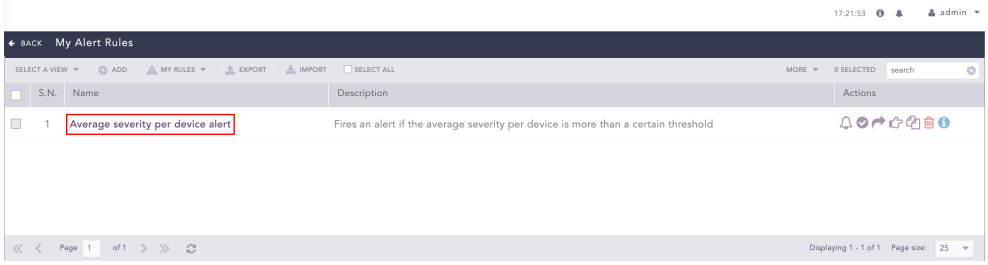
1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.



2. Click **IMPORT**.
3. Browse to the **Alert Rules**. You can only import alert rules exported from SLS with .pak extension.
4. Click **Submit**.

Editing an Alert Rule

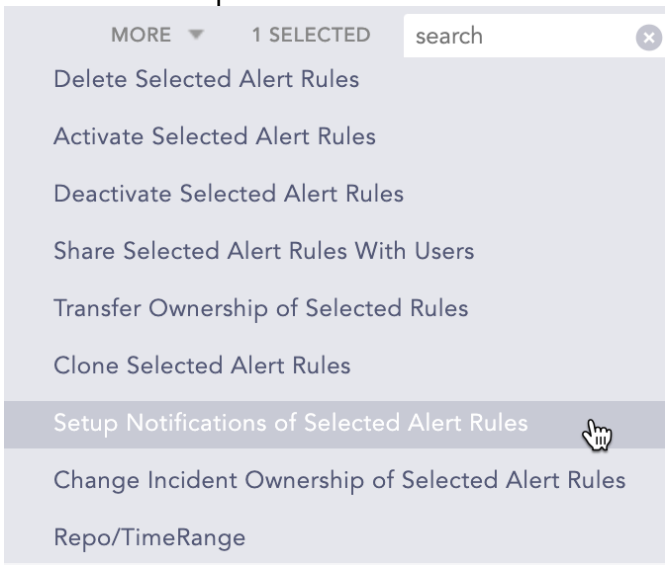
1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Click the **Name** of the alert rule that you want to edit.



3. Update the information.
4. Click **Submit**.

Editing Notification Configuration for multiple Alert Rules

1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Select the alert rules for which to setup notifications.
3. Click the **More** drop-down.

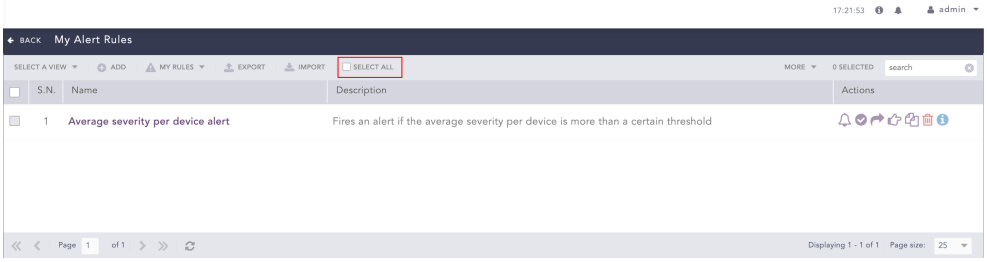


4. Select **Setup Notifications of Selected Alert Rules**.
5. Configure the notifications and click **Save**.

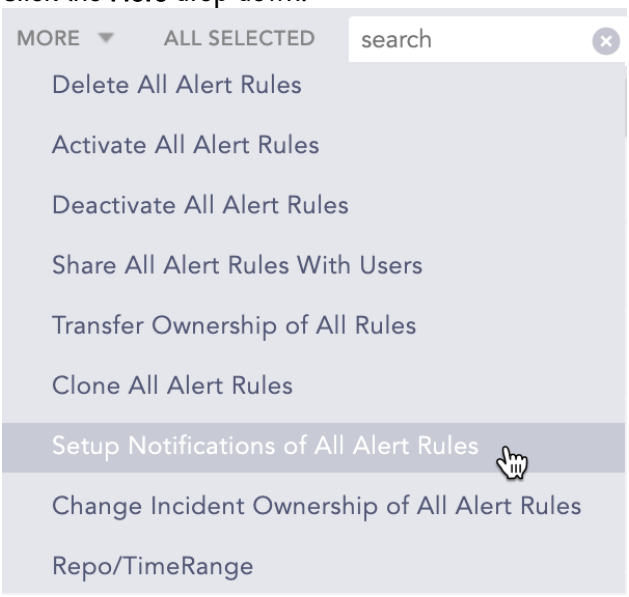
> **NOTE**
> By default, SLS updates only the alert rules that do not have the notifications configured. To update all the alert rules, select **Overwrite existing notifications**.

Editing Notification Configuration for all the Alert Rules

1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Click **Select All**.



3. Click the **More** drop-down.



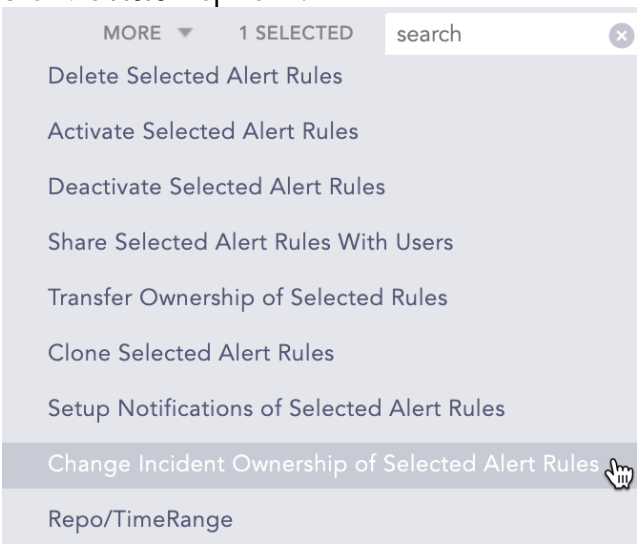
4. Select **Setup Notifications of All Alert Rules**.
5. Configure the notifications and click **Save**.

> **NOTE**
> By default, SLS updates only the alert rules that do not have the notifications configured. To update all the alert rules, select **Overwrite existing notifications**.

Editing Ownership for multiple Alert Rules

1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Select the alert rules to edit the ownership for.

3. Click the **More** drop-down.



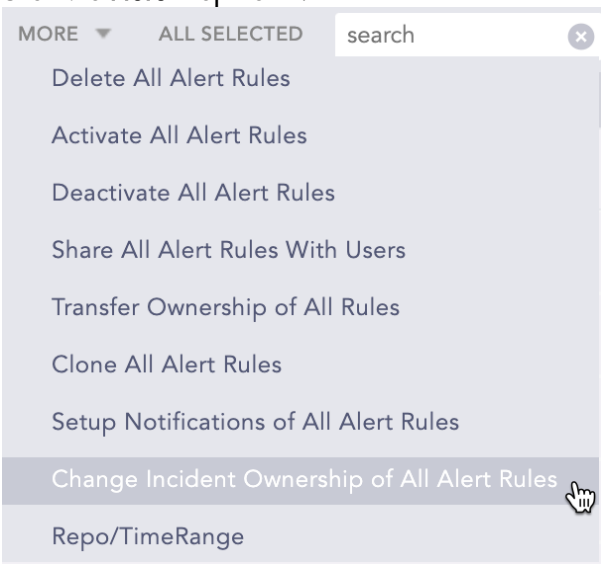
4. Select **Change Incident Ownership of Selected Alert Rules**.
5. Edit the ownership and click **Save**.

> **NOTE**
> By default, SLS updates only the alert rules that do not have the notifications configured. To update all the alert rules, select **Overwrite existing ownership**.

Editing Ownership for all the Alert Rules

1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Click **Select All**.

3. Click the **More** drop-down.

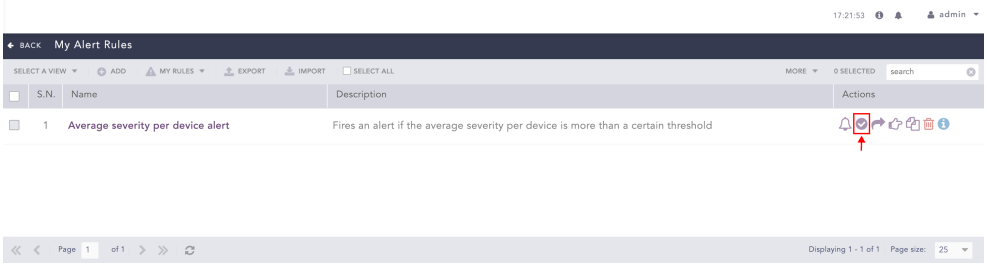


4. Select **Change Incident Ownership of All Alert Rules**.
5. Edit the ownership and click **Save**.

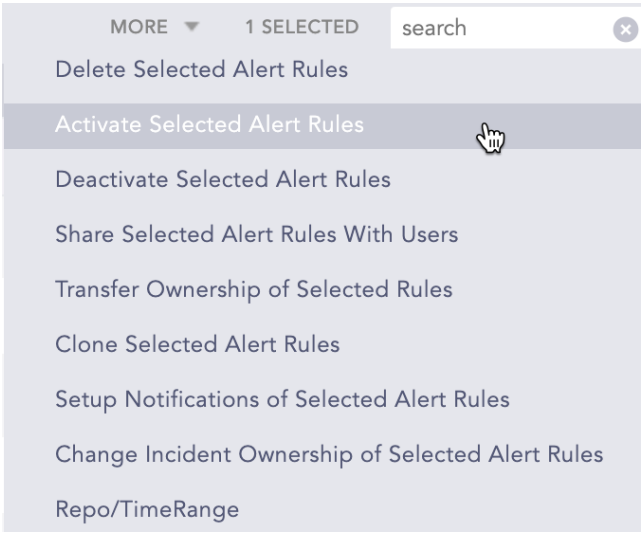
> **NOTE**
> By default, SLS updates only the alert rules that do not have the notifications configured. To update all the alert rules, select **Overwrite existing ownership**.

Activating Alert Rules

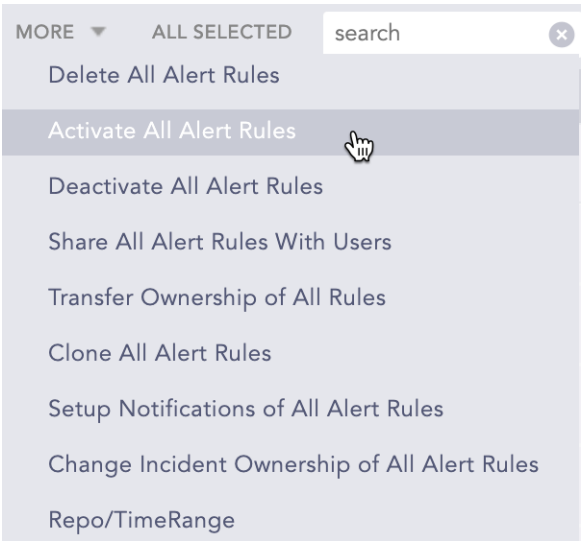
1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Click the **Activate alert rule** icon under the **Actions** column for the label package.



- To activate multiple alert rules, select the alert rules. Click the **More** drop-down and select **Activate Selected Alert Rules**.



- To activate all the alert rules, click **Select All**. Go to the **More** drop-down and select **Activate All Alert Rules**.



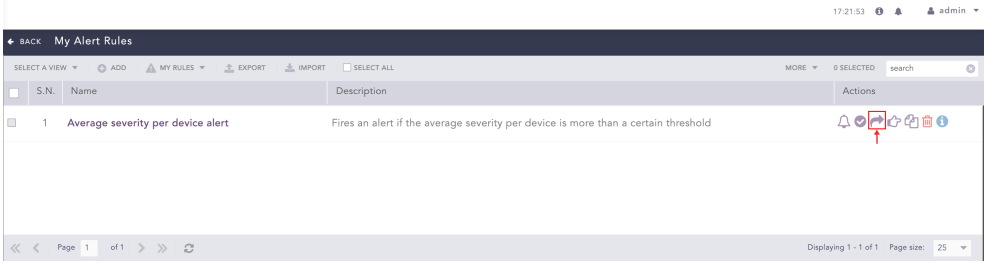
NOTE
You can **De-activate** the alert rules using the same method.

Sharing Alert Rules with Users

You can share alert rules with different users and give them read, edit, or full permissions. Incidents for each shared user and owner are triggered independently.

1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Select **My Rules** from the drop-down.

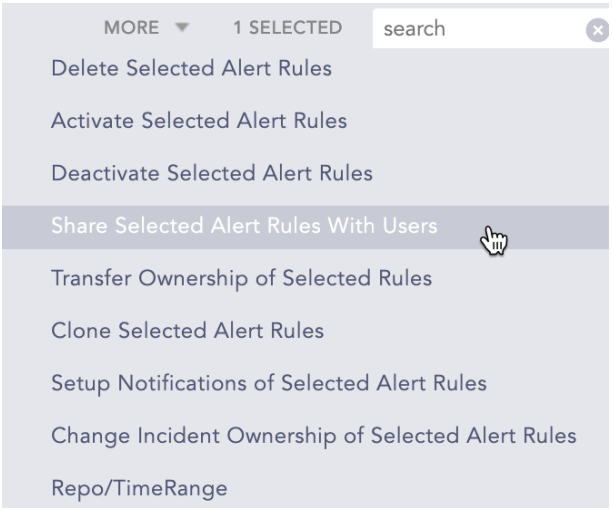
3. Click the **Share/Unshare to Other Users** icon under the **Actions** column for the alert rule.



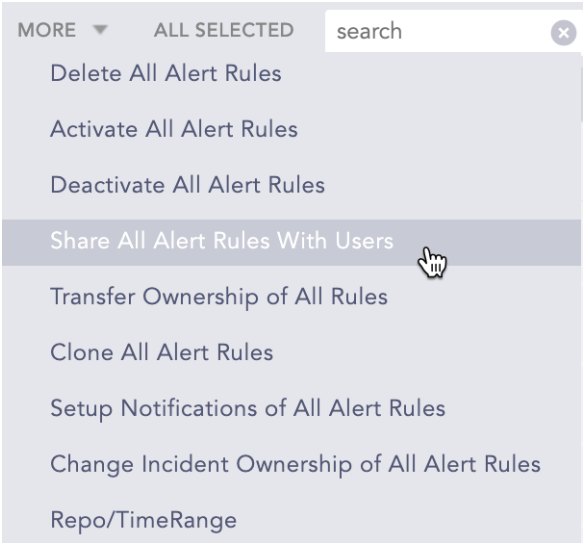
NOTE

The **Unshared. Click to Share** ( ) icon appears if you have not shared the alert rule previously.

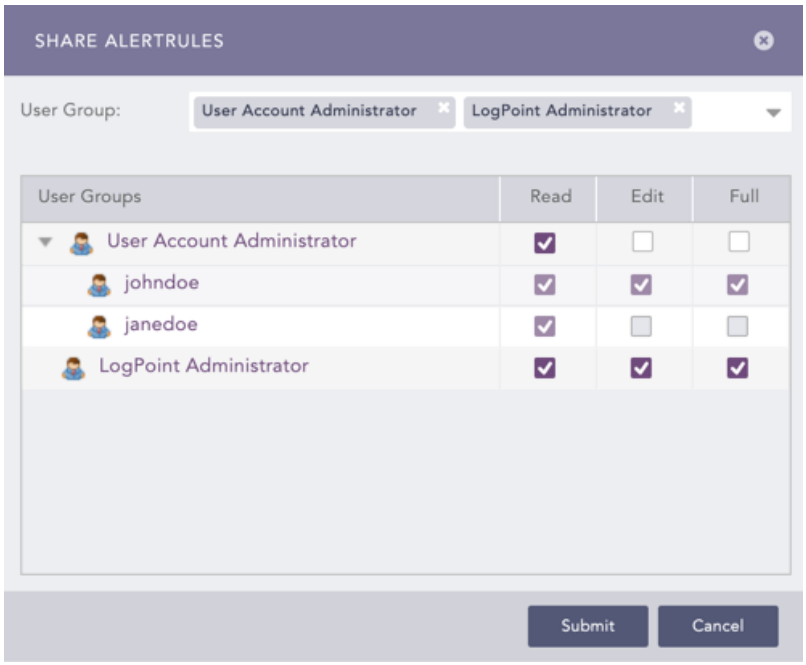
- To share multiple alert rules, select the alert rules. Click the **More** drop-down and select **Share Selected Alert Rules With Users**.



- To share all the alert rules, click **Select All**. Go to the **More** drop-down and select **Share All Alert Rules With Users**.



4. Select a **User Group**. All the users in the user group are listed in the drop-down.
5. Select **Read**, **Edit**, or **Full** permissions for the users. The read permission allows a user to use and clone the alert rules; the edit permission allows a user to use, clone, and edit the alert rules; and the full permission allows a user to use, clone, edit, remove, and share the alert rules.



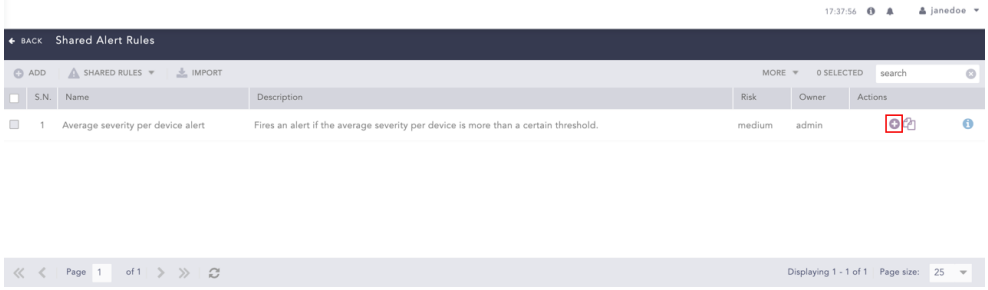
6. Click **Submit**

> **NOTE**
> You can unshare alert rules with the users using the same method.

Using Shared Alert Rules

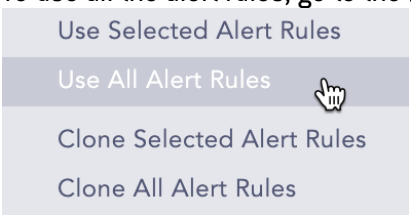
1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Select **Shared Rules** from the drop-down.

3. Click the **Use** icon under the **Actions** column.



- To use multiple alert rules, select the alert rules. Click the **More** drop-down and select **Use Selected Alert Rules**.

- To use all the alert rules, go to the **More** drop-down and select **Use All Alert Rules**.



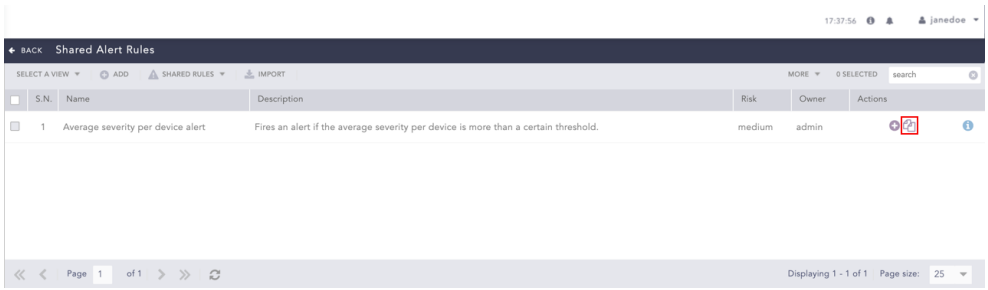
NOTE

- If a user does not have access to a repo used in a shared alert rule, the incident is triggered from other selected repos.
- If only one repo is selected in the shared alert rule, and the user does not have access to the repo, the incident is not triggered.

Cloning Shared Alert Rules

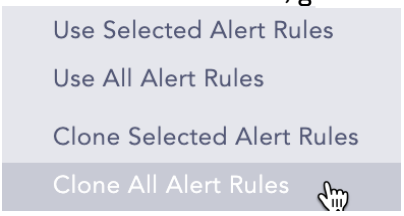
1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Select **Shared Rules** from the drop-down.

3. Click the **Clone** icon under the **Actions** column.



- To clone multiple alert rules, select the alert rules. Click the **More** drop-down and select **Clone Selected Alert Rules**.

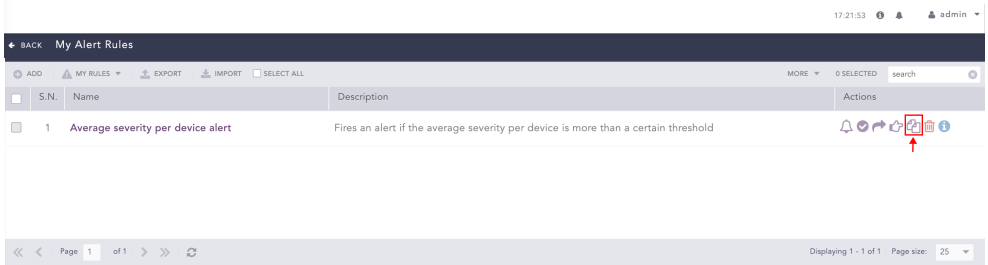
2. To use all the alert rules, go to the **More** drop-down and select **Clone All Alert Rules**.



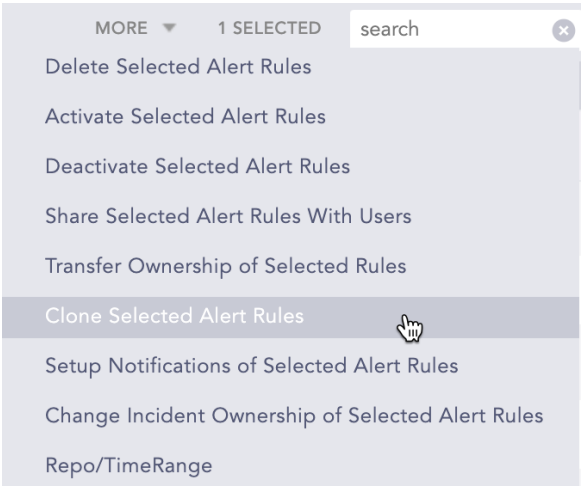
4. Enter a new **Name** for the cloned rule.
5. Select the **Replace Existing?** checkbox to replace an existing rule with the same name.
6. Click **Clone**.

Cloning Alert Rules

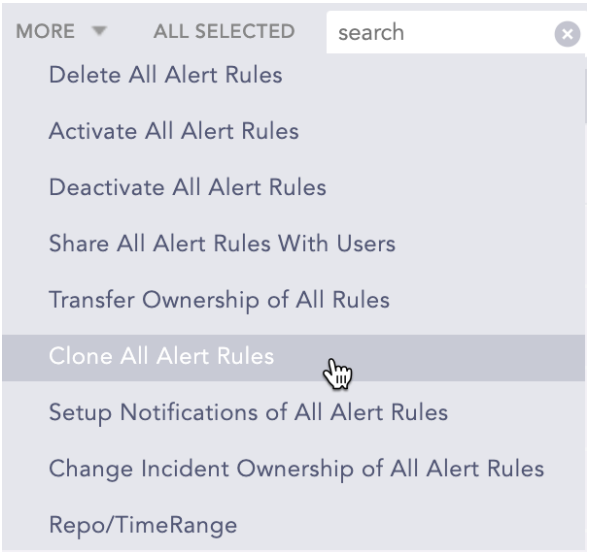
1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Click the **Clone Alert Rule** icon under the **Actions** column for the rule.



- To clone multiple alert rules, select the alert rules. Click the **More** drop-down and select **Clone Selected Alert Rules**.



- To clone all the alert rules, click **Select All**. Go to the **More** drop-down and select **Clone All Alert Rules**.



3. Enter a new **Name** for the cloned rule.
4. Check the **Replace Existing?** checkbox to replace an existing rule with the same name.
5. Click **Clone**.

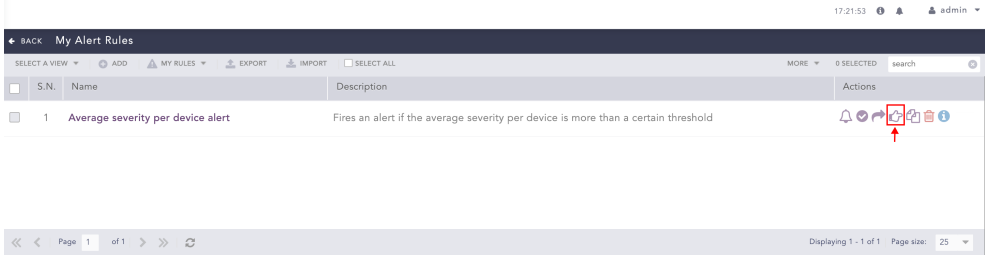
Transfer Ownership of Alert Rules

You can transfer alert rule ownership from one user to another. It is important to transfer alert rule ownership when a user who owns alert rules needs to be deleted. This is also relevant when a user becomes part of a different User Group and no longer needs to own the same alert rules.

To transfer the ownership of Alert Rules:

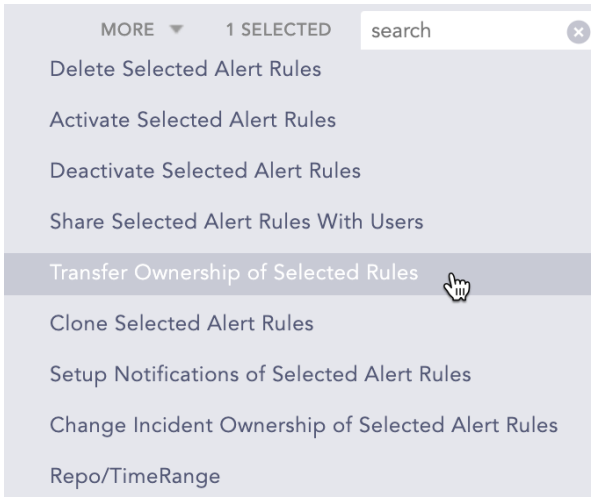
1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Click **My Rules** from the dropdown next to **+Add**.

3. Click the right hand pointer icon under the Actions column of the alert rule.

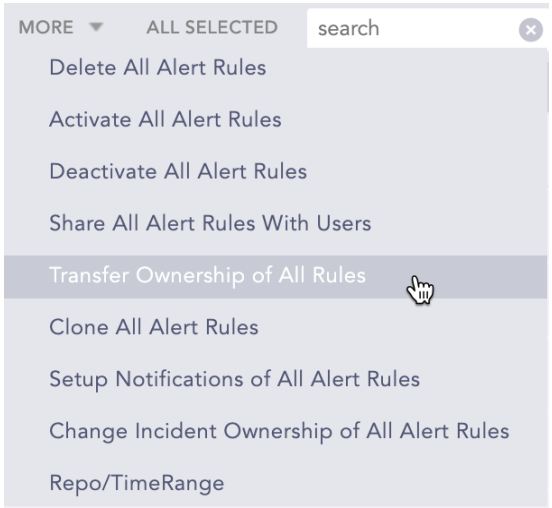


To transfer ownership:

- of multiple alert rules, select them. Click the More drop-down and select Transfer Ownership of Selected Rules.



- of all alert rules, click Select. Click the More drop-down and All select Transfer Ownership of All Rules.

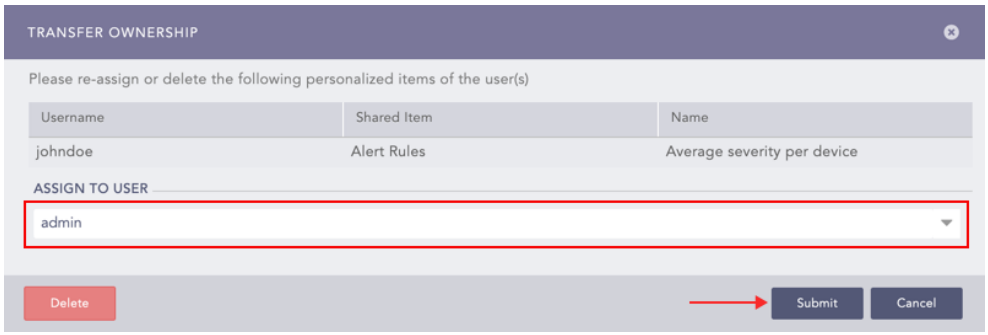


4. **Select a User** from the drop-down.
5. Click **OK**.
6. To view transferred alert rules, go to **Settings >> Knowledge Base >> Alert Rules**. Click the **USED RULES** dropdown and go to **Transferred Rules**.

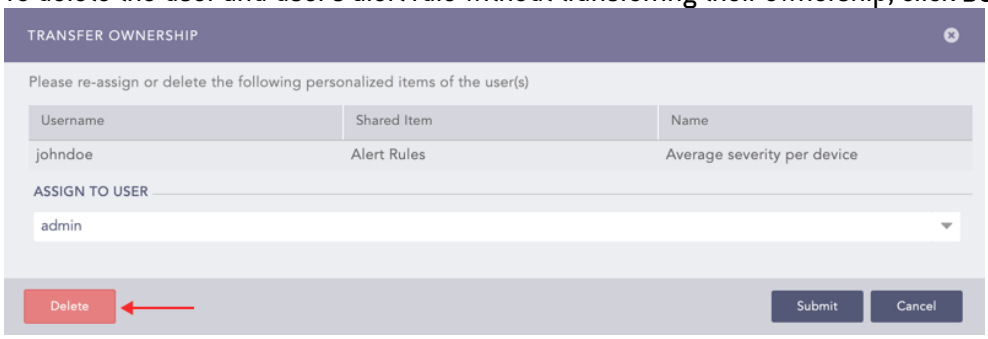
Transfer Ownership When Deleting Shared Alert Rule's Owner

When you delete a user who has shared alert rules you must delete the shared alert rule or transfer the alert rule's ownership to another user.

1. Go to `Settings >> User Accounts` from the navigation bar and click **Users**.
2. De-activate the user by clicking the **De-Activate User** icon under the **Actions** column.
3. Click **Manage De-Activated Users**.
4. Click the **Delete** icon under the **Actions** column of the user.
5. Click **Yes**.
6. To transfer the ownership, select a user from the list of active users in the drop-down and click **Submit**.

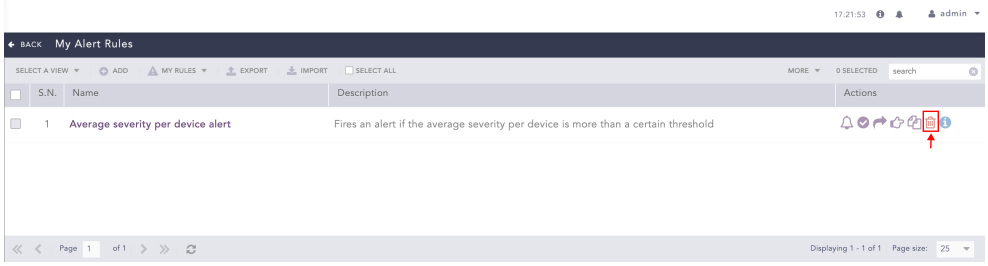


7. To delete the user and user's alert rule without transferring their ownership, click **Delete**.

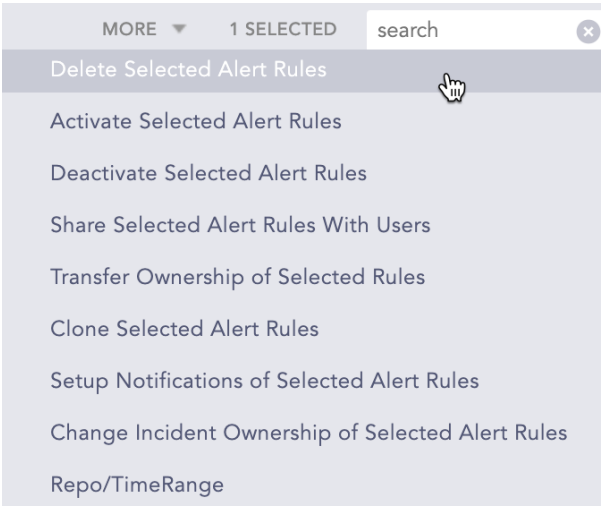


Deleting Alert Rules

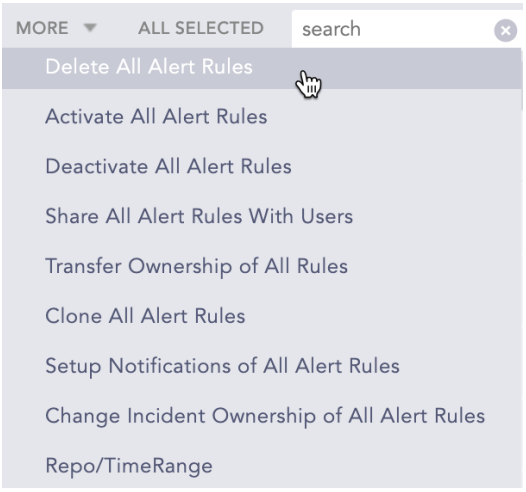
1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Click the **Delete** icon under the **Actions** column for the rule.



- To delete multiple alert rules, select the alert rules. Click the **More** drop-down and select **Delete Selected Alert Rules**.



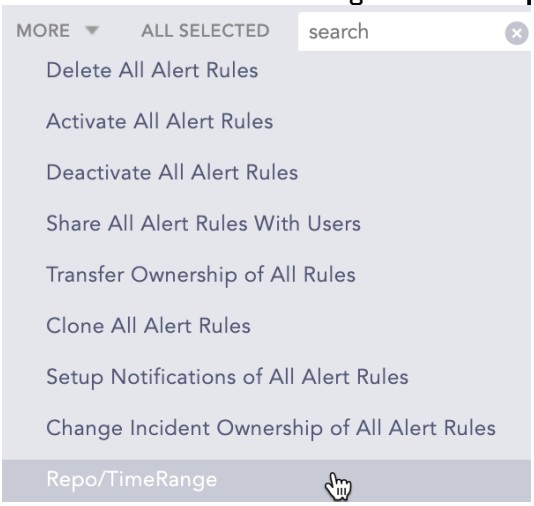
- To delete all the alert rules, click **Select All**. Go to the **More** drop-down and select **Delete All Alert Rules**.



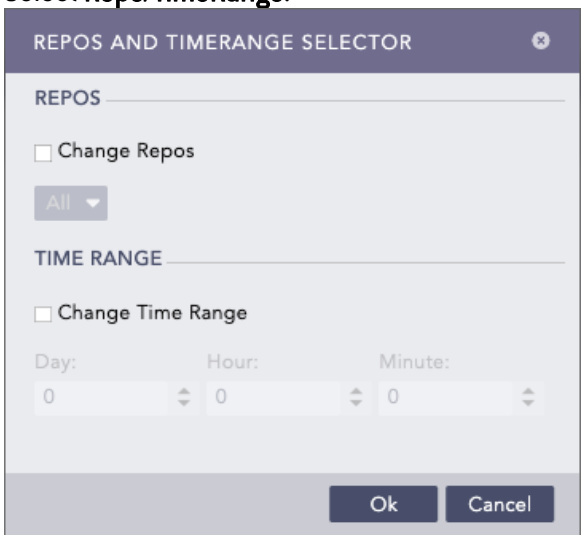
3. A delete confirmation dialog box appears on the screen. Click **Yes** to proceed.

Changing Time Range and Repo of Alert Rules

1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Select the **Alert Rules** to change the **Time/Repo** and click the **More** drop-down.



3. Select **Repo/TimeRange**.



4. Enable **Change Repos** and select the repos.
5. Enable **Change Time Range** and select the time range.
6. Click **Submit**.

SLS Reserved Jinja Placeholders

You can use the reserved Jinja placeholders in the SLS fields that support Jinja. You can use the Jinja placeholders as templates to customize the output of a subject, message, or view. Refer to Setting Up Alert Notifications and Creating an Alert Rule to know more about the Jinja supported fields of SLS.

Placeholders	Description
{{alert_name}}	Displays the name of the alert.
{{alertrule_id}}	Displays the ID of the alert.

Placeholders	Description
{{attack_category}}	Displays the attack category associated with the alert. This corresponds to the tactics in Mitre ATT&CK Framework.
{{attack_id}}	Displays the ID of the attack tags associated with the alert. This corresponds to the ID in Mitre ATT&CK Framework.
{{attack_tag}}	Displays the attack tag associated with the alert. This corresponds to the techniques and sub-techniques in Mitre ATT&CK Framework.
{{description}}	Displays the description of the alert.
{{detection_timestamp}}	Displays the Epoch time when the alert was triggered.
{{extra_info}}	Displays the information related to alert in a key-value format.
{{format}}	Displays the timestamp format of the alert according to Year, Month, Day, Hour, Minutes, and Seconds.
{{incident_id}}	Displays the ID of the incident generated by the alert.
{{loginspect_ip_dns}}	Displays the IP of the SLS where the alert was triggered.
{{sls_name}}	Displays the name of the SLS where the alert was triggered.
{{log_source}}	Displays the log sources associated with the alert.
{{risk_level}}	Displays the risk level of the alert.
{{rows}}	Displays the log messages that triggered the alert.
{{rows_count}}	Displays the total count of log messages that triggered the alert.
{{search_link}}	Displays the link to search for alert related log.
{{status}}	Displays the resolution status of incident generated by the alert.
{{time_range}}	Displays the time-range of the alert in Epoch time.
{{timezone}}	Displays the device timezone (UTC, GMT, ECT)
{{type}}	Displays the query type of the alert.
{{user_id}}	Displays the identity of the user account that triggered the alert.
{{_id}}	Displays the object ID of the incident generated by the alert.

NOTE
These are the publicly available Jinja placeholders. However, there are other SLS supported Jinja placeholders as well that are assigned for internal usage only.

Incidents

Incidents are used to identify, analyze, correct, and thereby prevent information hazards in the future. SLS lets you find events such as a system crash, power down, cables unplugged, high disk usage, high CPU usage, and forensics by creating incidents for each of them. Incidents can be created either on an ad-hoc basis from the search logs or by pre-defined alert rules. If you create an alert rule to detect system crashes, an alert is fired whenever the search results match the alerting criteria. SLS then creates the corresponding incident based on the alert rule. You can view the log source of an incident to determine if it was triggered by an alert rule or by a search query.

The severity level of an incident can be identified by the following colors:

S.N.	Severity Level	Color
1	Critical	Red
2	High	Purple
3	Medium	Blue
4	Low	Gray

Creating an Incident

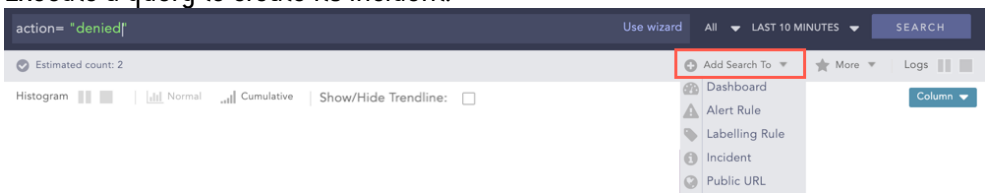
The methods of creating an incident are as follows:

- From Search Interface
- From Alert Rules
- From Widgets in Dashboards and Search Templates
- From the UEBA Anomalies Panel

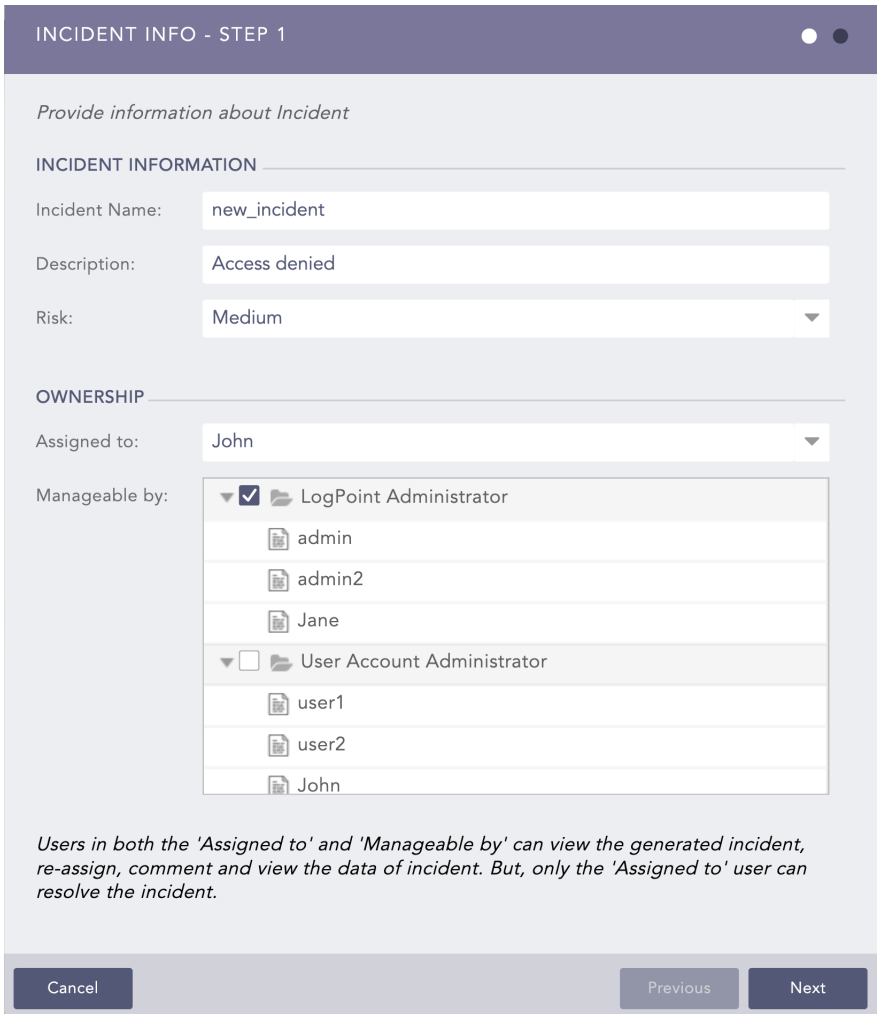
Creating Incident from Search Interface

You can create incidents for a particular search query from the Search Interface. Follow the instructions below to create incidents in this way.

1. Go to `Search` from the navigation bar.
2. Execute a query to create its incident.



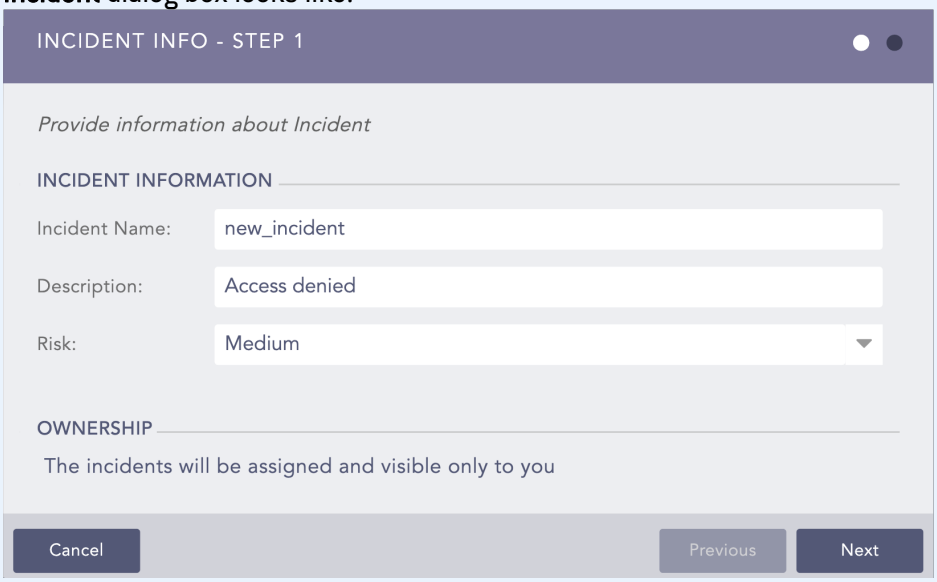
3. Go to the **Add Search To** drop-down and select **Incident** to open the **Create Search Incident Panel**.



4. Enter the **Incident Name**, and the **Description**.
5. Select a **Risk** level for the incident.
6. Select a user from the **Assigned to** drop-down to assign the ownership of the incident. The **Assigned to** drop-down displays all the distinct Users mapped to the **Incident User Groups** (via User Groups).
7. Choose a group(s) from the **Manageable by** tree node structure. The tree node structure displays all the **Incident User Groups** with their corresponding users present in the system. Users selected in both the **Assigned to** and **Manageable by** sections can view the generated incident, reassign it, and comment on the data. However, only the **Assigned to** user can resolve it.

NOTE

- While creating the incident, you can only see the **Assigned to** and the **Manageable by** sections if you belong to any of the **Incident User Groups**. Otherwise, the **Create Search Incident** dialog box looks like:



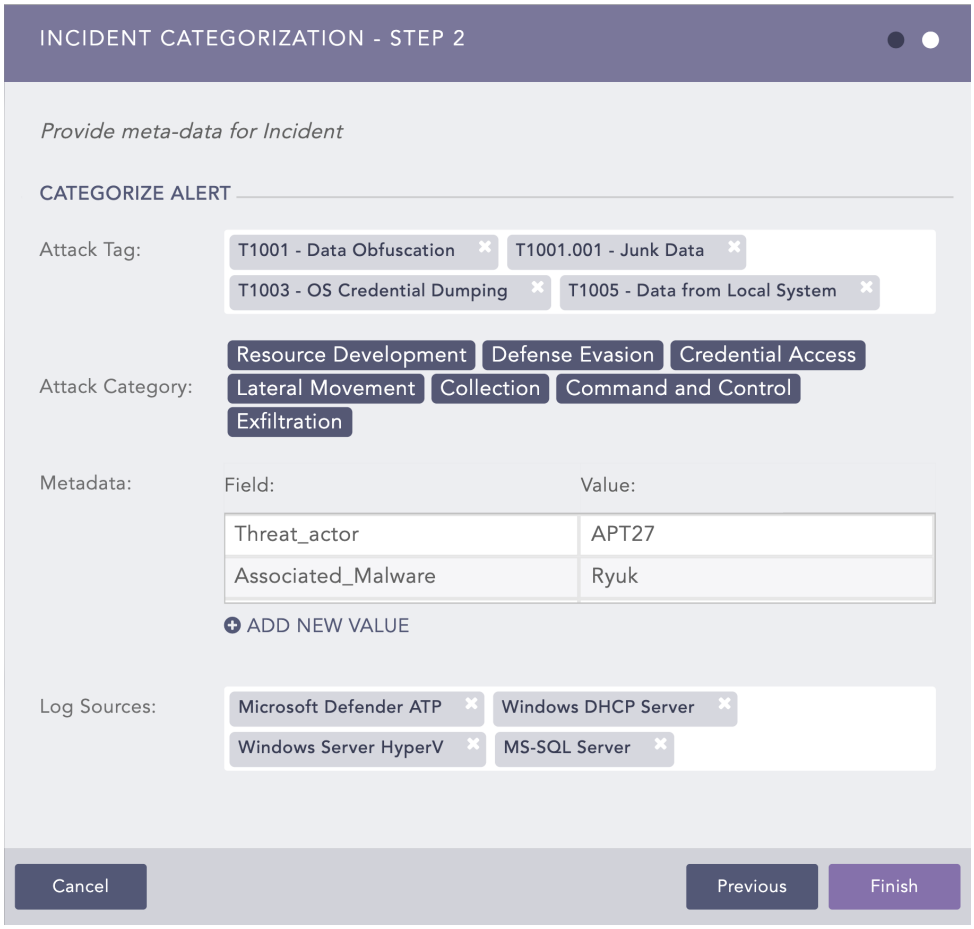
In this case, you are assigned to the generated incident, and you are responsible for managing it.

- If required, you can assign an incident to yourself and select none of the **Incident User Groups** from the **Manageable by** tree node structure.

8. Click **Next**.

NOTE

- The **Assigned to** and the **Manageable by** sections appear the same to the LDAP Users.
- The Alert Rule/Incident creators can see the incidents generated even if they are not present in the **Assigned to** drop-down and the **Manageable by** tree node structure.

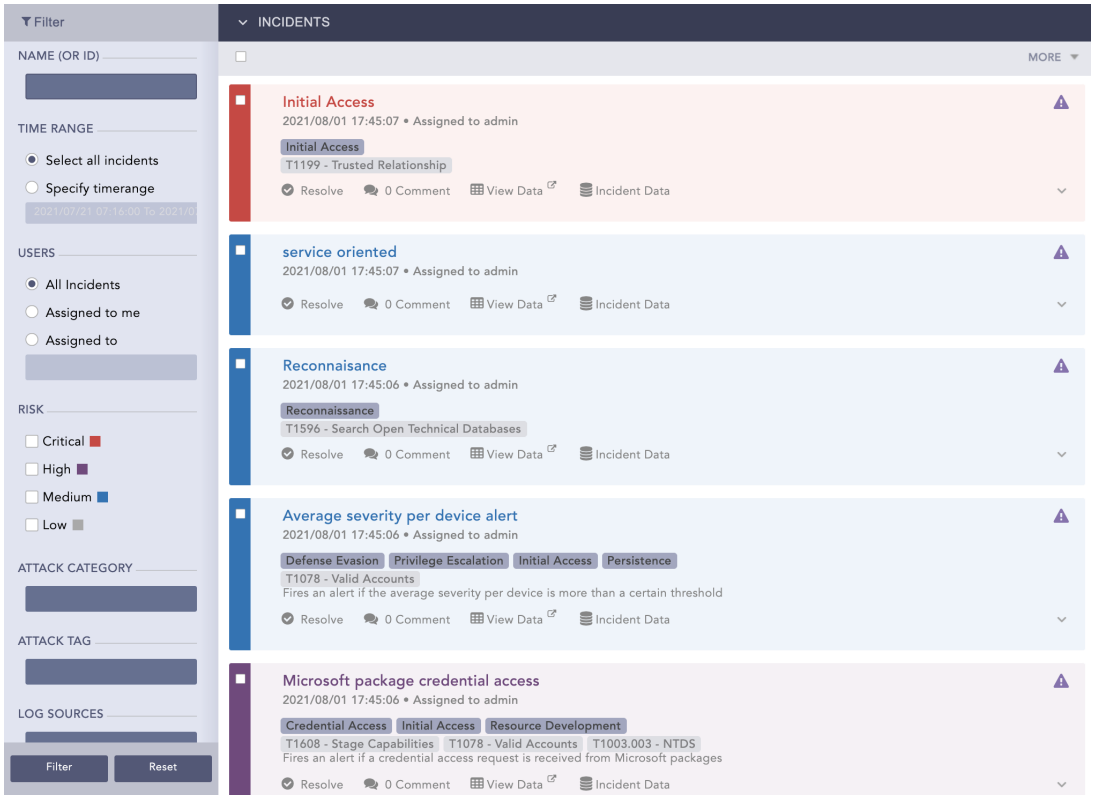


9. Select the **Attack Tag** from the drop-down. You can select multiple tags to categorize the incidents. **Attack Category** is selected based on the associated **Attack Tags** selected.
10. Provide custom **Metadata** as **Field** and **Value** to categorize the incidents. You can add new fields and values by clicking the **ADD NEW VALUE** button.

IMPORTANT

- You cannot provide SLS reserved Jinja placeholders as Metadata Field in the **Field** column. Refer to `SLS Reserved Jinja Placeholder` to view the list of publicly available SLS reserved Jinja placeholders.
- The Metadata Field should contain letters or a combination of letters, numbers, or underscores (_), and must start with a letter.
- You cannot repeat the Metadata Field.
- Value associated with the Metadata Field cannot be empty and vice-versa.

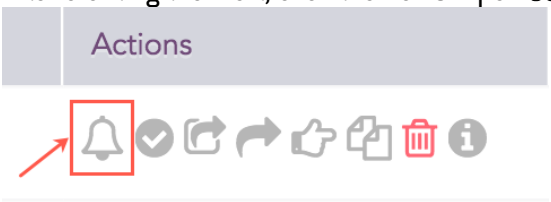
11. Select **Log Sources** from the drop-down or provide new log sources associated with the alert rule. New log sources are also updated in the drop-down after submission.
12. Click **Finish**. As soon as this form is successfully submitted, a new incident is generated and populated on the Incident page. You can access the Incident page under `Investigation >> Incidents` from the navigation bar.



Creating Incident from Alert Rule

The purpose of an alert rule is to monitor data continuously. Once SLS finds the search result matching an alert, it fires the corresponding incidents. The process of creating an incident from alert rules is given below:

1. Go to `Settings >> Knowledge Base` from the navigation bar and click **Alert Rules**.
2. Create an alert rule on the basis of your requirements. For details, refer to the Creating an Alert Rule section.
3. After creating the alert, click the bell shaped **Setup Notification** icon in the **Actions** column.

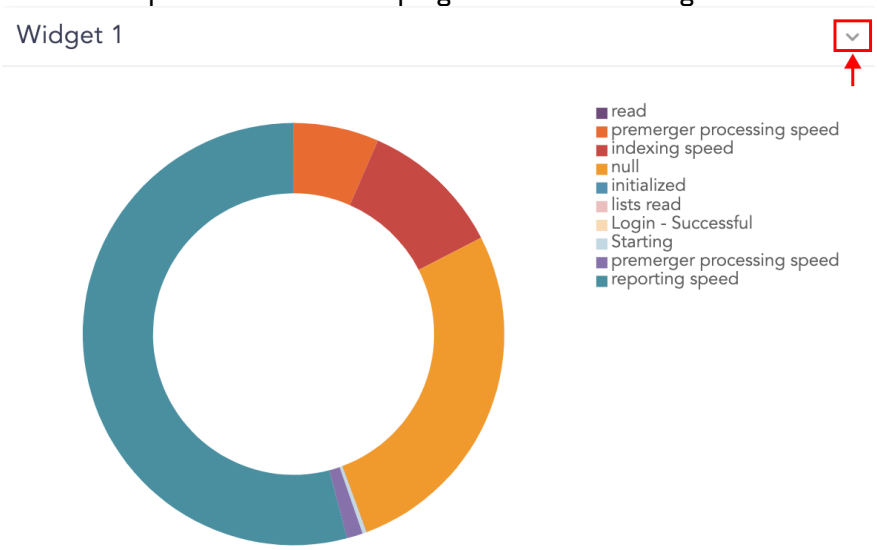


4. Choose the type of notification you would like to configure and fill in their respective required parameters. Refer to the Setting Up Alert Notifications section for the detailed information.
5. Click **Save**.

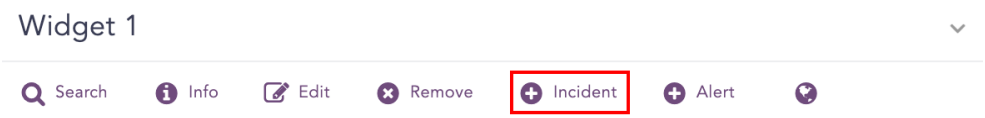
After creating the alert rule, the incidents of the corresponding alerts fired are automatically generated and populated in the Incident menu.

Creating Incident from the Widgets in Dashboards and Search Templates

1. Go to the dashboard or search template containing the required widget.
2. Click the drop-down icon at the top-right corner of the widget.



3. Click **Incident**.



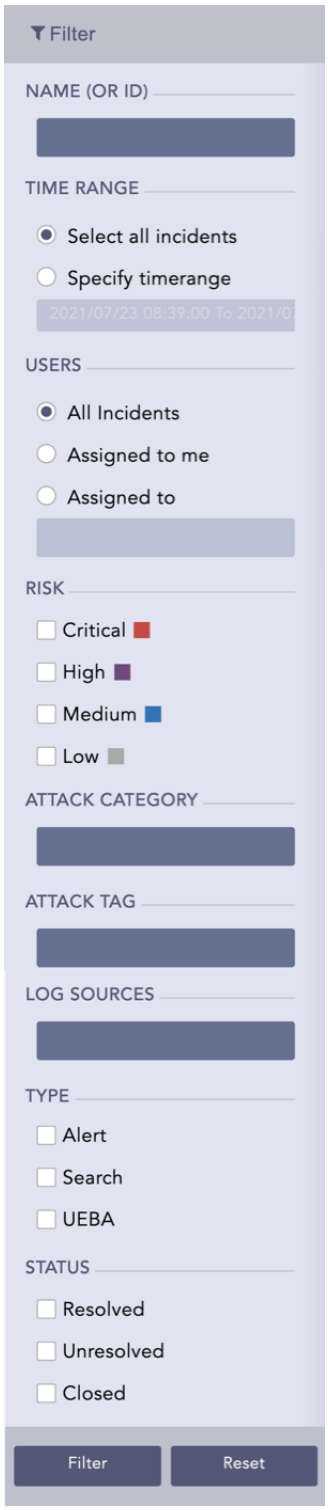
4. Enter the relevant data and **Submit** the form.

> **NOTE**
> Refer to the Creating Incident from Search Interface section for details on filling out the form.

Creating Incident from the UEBA Anomalies Panel

Only the SLS UEBA users can create incidents using this method.

Filtering an Incident



The devices may trigger multiple incidents which would make searching for a particular incident complicated. To narrow down the search for a particular incident, you can use various filters such as **Name (OR ID)**, **TimeRange**, **Users**, **Risk**, **Attack Category**, **Attack Tag**, **Log Sources**, **Type**, and **Status**.

You can access the Incident page and its filter under `Investigation >> Incidents` from the navigation bar.

You can directly search for a particular incident by specifying its name or its **Incident ID**. You can also search for all the incidents associated with an alert using the **AlertRule ID**.

You can obtain the **Incident ID** and **AlertRule ID** by clicking the `Incident Data` option on the Incident page. You can also use the following filters to search for specified incidents.

1. **TimeRange**: to view the incidents generated at a particular time.
2. **Users**: to view the incidents assigned to you or any other users.
   - When you select the **All Incidents** option, the incidents created by, assigned to and manageable by the current user (the user who has logged in) are listed.
3. **Risk**: to view the incidents of a particular severity level (critical, high, medium, low).
4. **Attack Category**: to view the incidents according to the attack categories associated. You can select multiple attack categories from the drop-down.
5. **Attack Tag**: to view the incidents according to the attack tags associated. You can select multiple attack tags from the drop-down.
6. **Log Sources**: to view the incidents according to the log sources associated. You can select multiple log sources from the drop-down.
7. **Type**: to view the incidents by the source (Alert, Search, UEBA) that generated them.
8. **Status**: to view the incidents according to their status (resolved, unresolved, closed).

Incident Actions

In the Incident page, you can find the list of all the incidents along with their states and the attack tags and attack categories associated with them. You can **Resolve**, **Re-open**, **Close**, **Comment** on, and **View the Data** for these incidents. Additionally, you can send incident

notifications for investigation if you have configured the **Manual** notification trigger for the corresponding alert rules.

Resolve

Once appropriate action(s) has been taken on a particular incident, you can **Resolve** it.

Re-open

If you feel that an incident has not been satisfactorily resolved even after it was closed, you can re-open it. This can be done by clicking **Re-open** on the particular incident.

Close

After an incident is resolved and needs to be close, you can close it by clicking on the **Close** option. Once an incident is closed, it is not shown in the incident page. However, it can easily be retrieved using the **Closed** option in the **Status** filter.

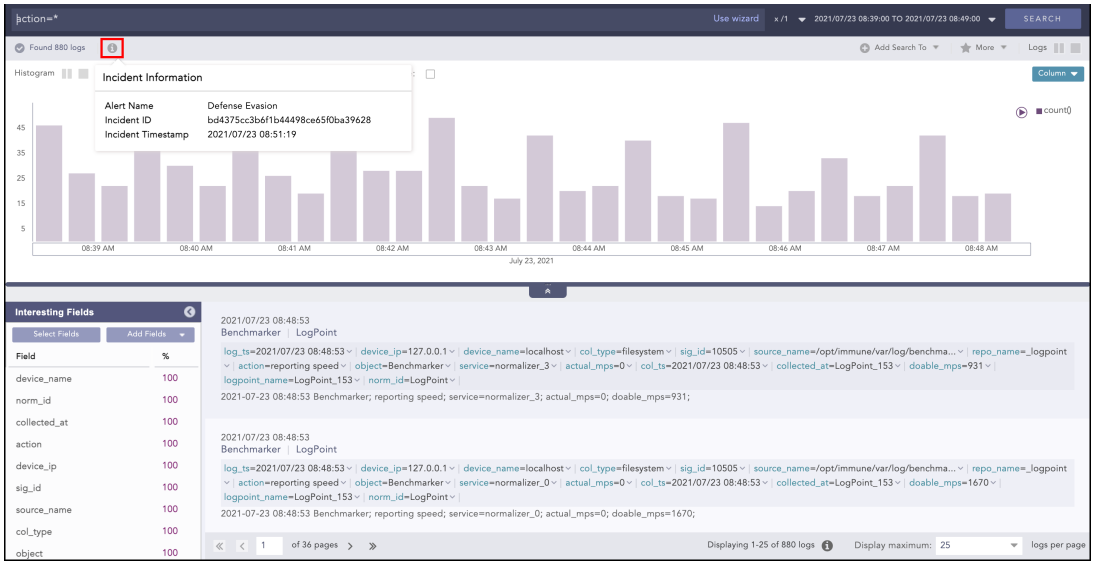
Comment

You can post comments on the incidents seen in the incident page. You can also track the actions taken over the incidents via the comments.

View Data

The **View Data** option directs you to the search page and shows the log messages that triggered the incident. You can click the **Open in new tab** ( ) icon to view the incident data in a new browser tab.

NOTE
You can view the incident information like Alert Name, Incident ID, and Incident Timestamp from the Incident Info ( ) icon on the redirected tab.



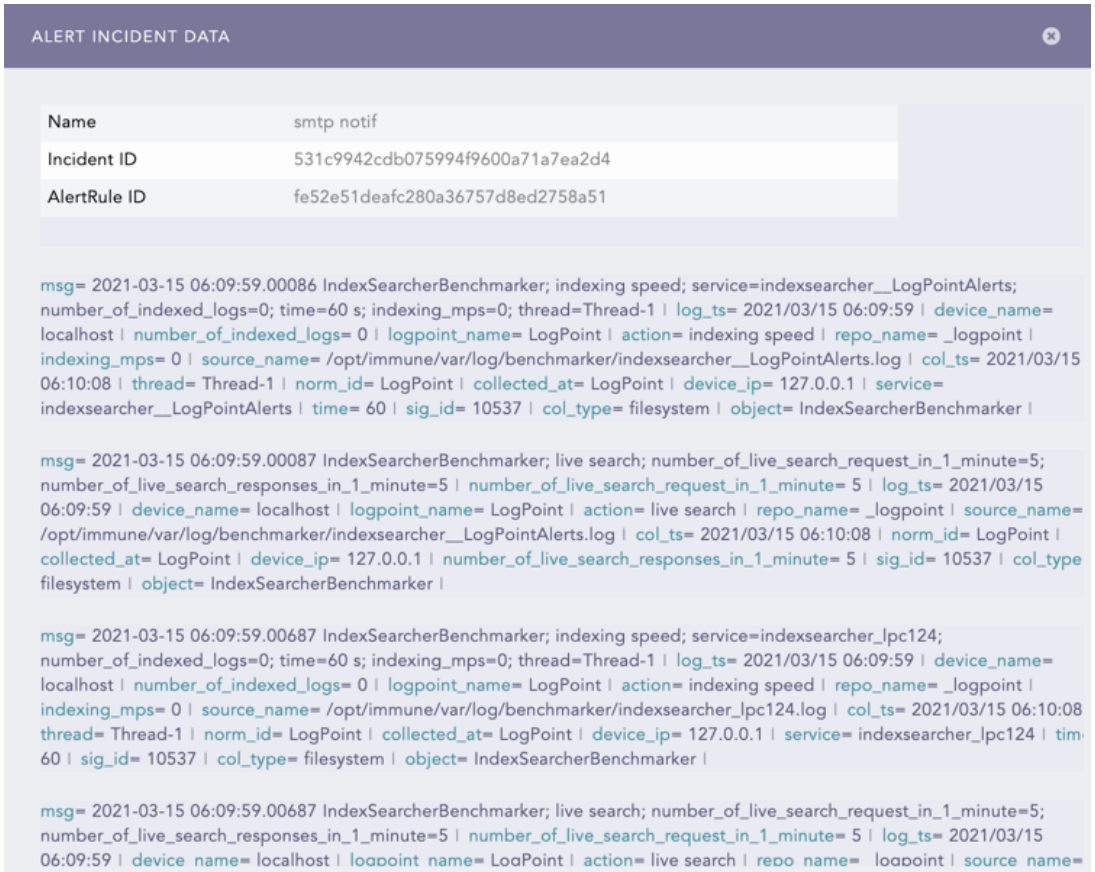
Incident Data

The **Incident Data** option opens a pop-up panel to display the data of the incident in the format specified in the **Incident Data View** panel while creating the alert rule.

NOTE
If the format was not specified in the **Incident Data View** panel while creating the alert rule, the **Incident Data** panel displays the logs of the generated incident.

You can monitor each incident's status using the **Incident ID**, which is a unique ID of an incident. It is constant for each incident. You can also view the corresponding AlertRule's **AlertRule ID** and search for all the incidents associated with an alert using the **AlertRule ID**.

NOTE
An **AlertRule ID** is only available in incidents generated from an alert.



Assign to me

The **Assign to me** option assigns the incident to you (the user who is logged in).

Send For Investigation

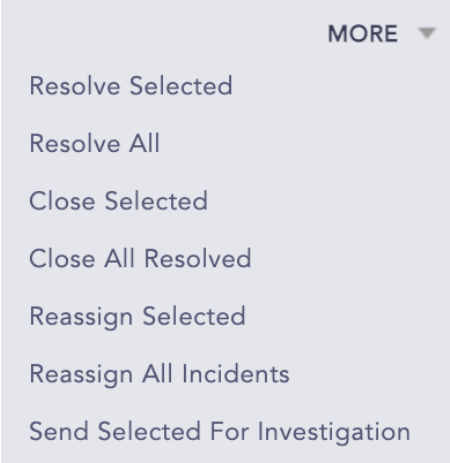
The **Send For Investigation** and **Re-Send For Investigation** options let you manually send incident notifications for further investigation.

NOTE

- The **Send For Investigation** and **Re-Send For Investigation** options only appear if one of the notifications has been set to trigger **Manually** in the corresponding alert rule.
- When you click **Send For Investigation**, only the notifications configured with the **Manual** trigger for the corresponding alert rule are sent.
- Incidents generated from Search, Dashboard, Search template, and UEBA can also be sent for investigation manually. The **Send For Investigation** and **Re-Send For Investigation** options are not available for these incidents. You can use the **Send Selected For Investigation** option under the **More** drop-down to send the incident(s) for investigation.

More

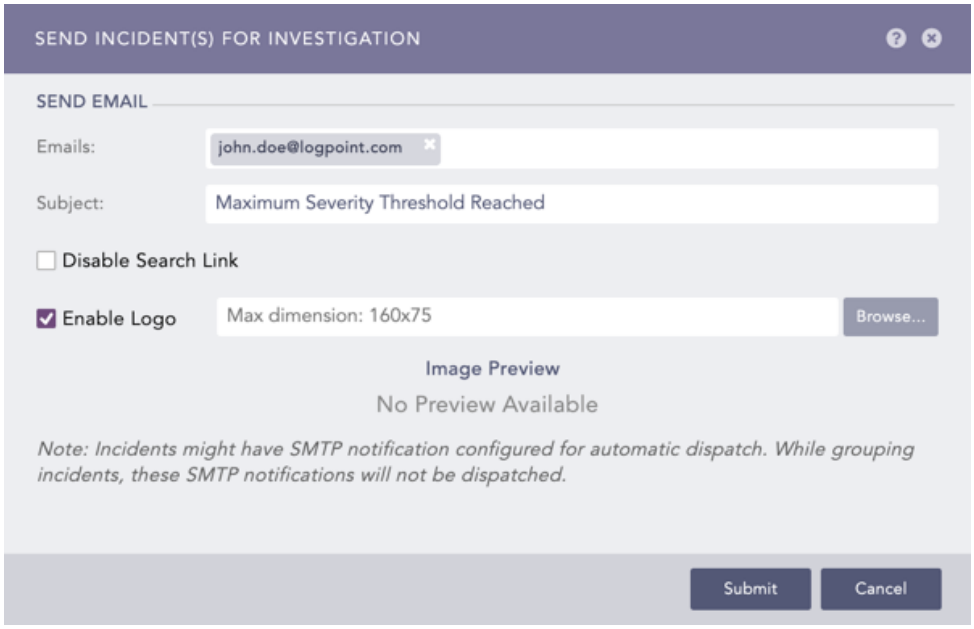
The **More** drop-down near the top-right corner of the Incident page lists additional actions.



- The **Resolve Selected** and **Resolve All** options let you resolve multiple incidents at once.
- The **Close Selected** and **Close All Resolved** options let you close multiple incidents at once.

NOTE
The incidents **cannot** be closed without being resolved first.

- The **Reassign Selected** and **Reassign All Selected** options let you reassign multiple incidents at once. Reassigning opens a window prompting you to select a user to reassign the incidents to.
- The **Send Selected For Investigation** option lets you send the notifications configured for the selected incidents. You can either select a single incident or multiple incidents and send them in an email using the **Send Incident(s) for Investigation** dialog box.



1. Provide valid email addresses under **Emails**.
2. Enter a **Subject**.
3. Select **Disable Search Link** to remove the search link in the email. The search link redirects you to the search page of the SLS instance from which the email notification is configured.
4. Select **Enable Logo** if you want to include the SLS logo in the email notification.
5. **Browse** for the image in JPG/JPEG format if you want to provide a custom logo. The maximum dimension for the custom logo is 160*75.
6. Click **Submit**.

NOTE

- If you do not want to include the SLS logo in the email, deselect **Enable Logo** and click **Submit**.
- Any pre-configured settings for email notification are replaced with the configurations set in the **Send Incident(s) for Investigation** dialog box for the particular instance.
- You must configure the **SMTP** service before sending email notifications.
- Only the incidents corresponding to the alert rules configured for manual trigger in email notification are sent in email.

Further reading

Additional information and answers to questions you may have about SLS are available in the Stormshield knowledge base (authentication required).

documentation@stormshield.eu