How-To Guide

# Configure Detection Rule in the Netsurion Open XDR platform

**Publication Date:**

March 30, 2023

## Abstract

The purpose of this document is to aid the Netsurion Open XDR platform administrators to configure and utilize the Detection Rules feature introduced in the version 9.4.

**Note:**

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

## Audience

This guide is for all the Netsurion Open XDR platform users who adapts to the Netsurion Open XDR platform version 9.4.

## Product Terminology

The following are the terms used throughout this guide:

- The term “Netsurion’s Open XDR platform” or “the Netsurion Open XDR platform” or “the Open XDR platform” refers to EventTracker.
- The term “Data Source Integrations” refers to Knowledge Packs.
- The term “Sensor” refers to Agent.

# Table Of Contents

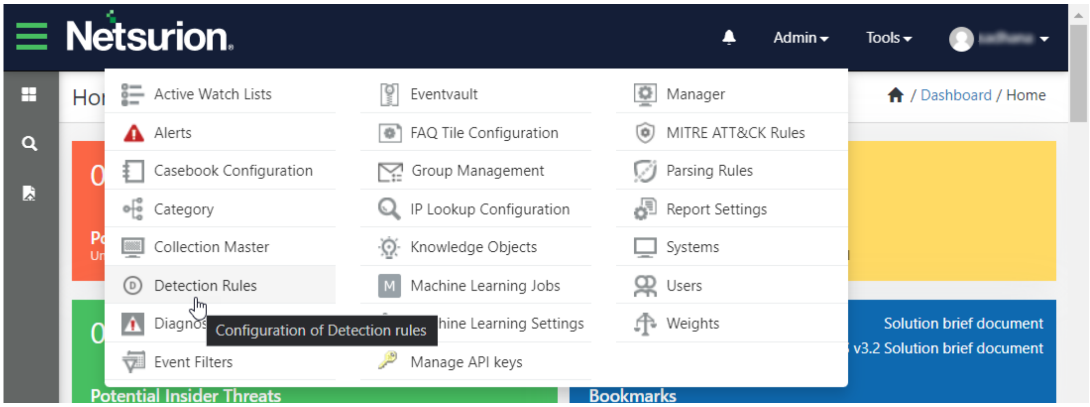
# 1 Detection Rules

The Detection Rules feature facilitates configuring rules for the attack pattern or technique detected from the MITRE ATT&CK framework, which triggers "tip-off" alerts based on certain criteria when the set threshold is exceeded. This reduces the false positives to a greater extend and eases to notify the users directly to the end point where the attack occurred. This feature also supports detection rules based on EventTracker index.

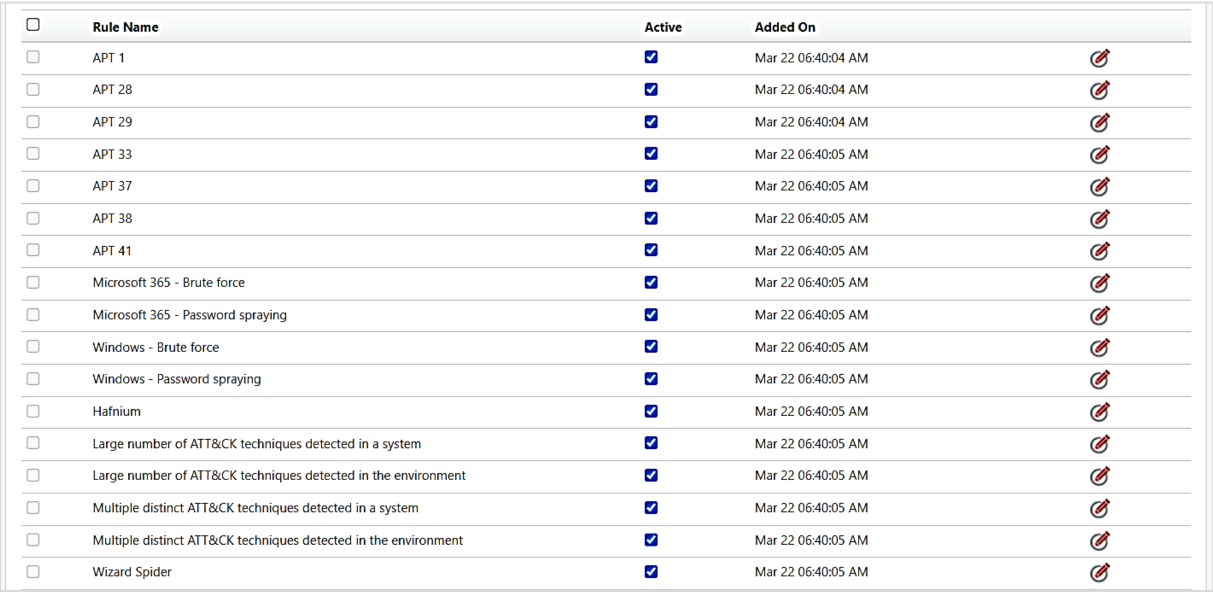
In the **Open XDR platform**, hover over the **Admin** menu and click **Detection Rules** to view all the configured detection rules.

**IMPORTANT:**

The Detection Rules feature is accessible only when the MITRE ATT&CK feature license is available on the console.



There are certain rules available by default (termed as Built-in rules) and each built-in rule can potentially trigger an alert with the details of the various attacks and techniques. The triggering threshold set varies based on the type of attack detections configured for each rule. The Netsurion Open XDR platform's administrator can also include additional custom rules (termed as user-defined rules) as per the requirement.



| ☐ | Rule Name | Active | Added On | |
|---|---|---|---|---|
| ☐ | APT 1 | ☑ | Mar 22 06:40:04 AM | |
| ☐ | APT 28 | ☑ | Mar 22 06:40:04 AM | |
| ☐ | APT 29 | ☑ | Mar 22 06:40:04 AM | |
| ☐ | APT 33 | ☑ | Mar 22 06:40:05 AM | |
| ☐ | APT 37 | ☑ | Mar 22 06:40:05 AM | |
| ☐ | APT 38 | ☑ | Mar 22 06:40:05 AM | |
| ☐ | APT 41 | ☑ | Mar 22 06:40:05 AM | |
| ☐ | Microsoft 365 - Brute force | ☑ | Mar 22 06:40:05 AM | |
| ☐ | Microsoft 365 - Password spraying | ☑ | Mar 22 06:40:05 AM | |
| ☐ | Windows - Brute force | ☑ | Mar 22 06:40:05 AM | |
| ☐ | Windows - Password spraying | ☑ | Mar 22 06:40:05 AM | |
| ☐ | Hafnium | ☑ | Mar 22 06:40:05 AM | |
| ☐ | Large number of ATT&CK techniques detected in a system | ☑ | Mar 22 06:40:05 AM | |
| ☐ | Large number of ATT&CK techniques detected in the environment | ☑ | Mar 22 06:40:05 AM | |
| ☐ | Multiple distinct ATT&CK techniques detected in a system | ☑ | Mar 22 06:40:05 AM | |
| ☐ | Multiple distinct ATT&CK techniques detected in the environment | ☑ | Mar 22 06:40:05 AM | |
| ☐ | Wizard Spider | ☑ | Mar 22 06:40:05 AM | |

**Note:**

The built-in rules include 13 MITRE ATT&CK index-based detection rules and 4 EventTracker index-based detection rules.

**Note:**

The Rule configuration for the built-in rules cannot be modified. The Netsurion Open XDR Administrator can 'Deactivate' a specific rule if needed to avoid any alert for that specific rule.

## UI Conventions

| | |
|---|---|
| ⊕ | Click to add a new Rule configuration |
| 🗑 | Select the required Rule name from the list and click to delete the existing Rule configuration from the list. |
| ⤓ | Click to import a Rule configuration to the system.<br>**Note:**<br>Refer Importing a Rule Configuration section for more details. |
| ⤒ | Select the required Rule name from the list and click to export a Rule configuration.<br>**Note:**<br>Refer Exporting a Rule Configuration section for more details. |
| ‹ 1 of 1 › | Click ‹ or › to navigate to the Back or the Front page in the Detection Rule interface. |
| ‹ 1 of 1 › GO | Click GO to go to the specified page. |
| Search... | Use the search field to search for a specific Detection Rule name |
| Activate Now | Click **Activate Now** to activate all the latest modifications |

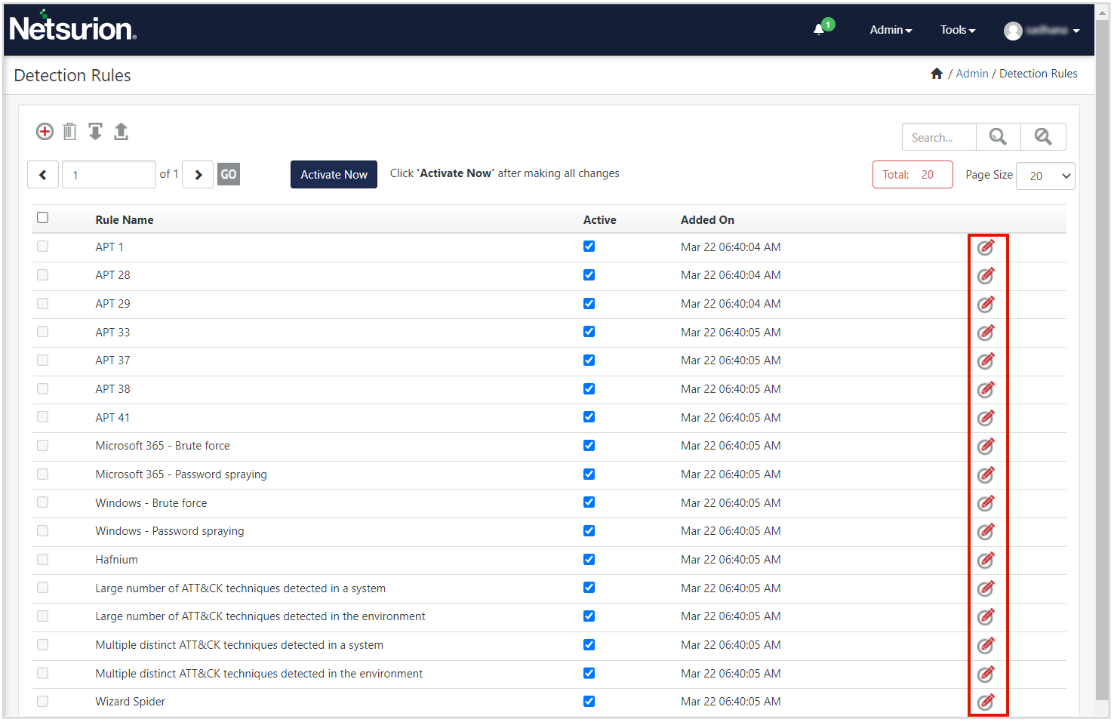
## 1.1 Modifying the Alert for the Built-in Rules

The Rule configuration for the Built-in rules cannot be modified but, the administrator can decide to trigger or stop the alert for the Built-in rules.

**Note:**

By default, the alerts for the Built-in rules will be triggered.

1. In the **Detection Rules** interface, click the **Edit** button of the Built-in rule for which you require to trigger or stop the alert.

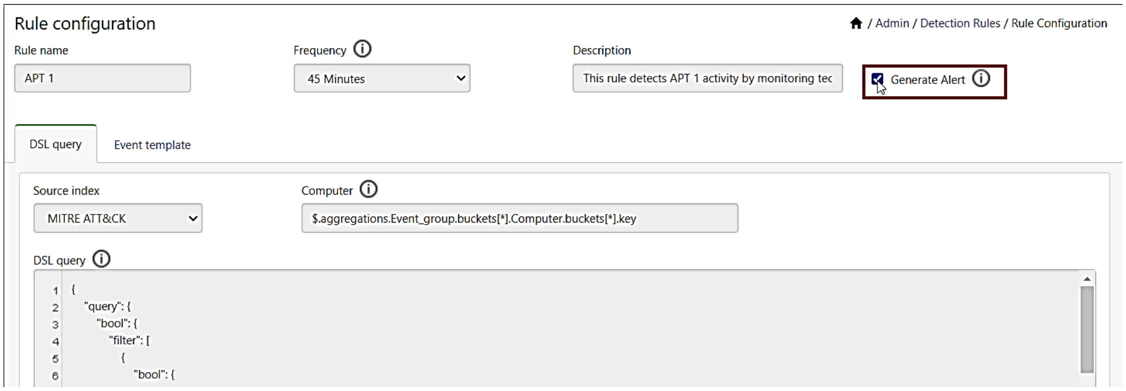


| □ | Rule Name | Active | Added On |
|---|---|---|---|
| □ | APT 1 | ☑ | Mar 22 06:40:04 AM |
| □ | APT 28 | ☑ | Mar 22 06:40:04 AM |
| □ | APT 29 | ☑ | Mar 22 06:40:04 AM |
| □ | APT 33 | ☑ | Mar 22 06:40:05 AM |
| □ | APT 37 | ☑ | Mar 22 06:40:05 AM |
| □ | APT 38 | ☑ | Mar 22 06:40:05 AM |
| □ | APT 41 | ☑ | Mar 22 06:40:05 AM |
| □ | Microsoft 365 - Brute force | ☑ | Mar 22 06:40:05 AM |
| □ | Microsoft 365 - Password spraying | ☑ | Mar 22 06:40:05 AM |
| □ | Windows - Brute force | ☑ | Mar 22 06:40:05 AM |
| □ | Windows - Password spraying | ☑ | Mar 22 06:40:05 AM |
| □ | Hafnium | ☑ | Mar 22 06:40:05 AM |
| □ | Large number of ATT&CK techniques detected in a system | ☑ | Mar 22 06:40:05 AM |
| □ | Large number of ATT&CK techniques detected in the environment | ☑ | Mar 22 06:40:05 AM |
| □ | Multiple distinct ATT&CK techniques detected in a system | ☑ | Mar 22 06:40:05 AM |
| □ | Multiple distinct ATT&CK techniques detected in the environment | ☑ | Mar 22 06:40:05 AM |
| □ | Wizard Spider | ☑ | Mar 22 06:40:05 AM |

2. The Rule configuration details for the selected Built-in rule will be displayed. Select or clear the selection of the **Generate Alert** check box to trigger or stop the alert for that particular Built-in rule.

**Note:**

You cannot edit any of the Rule Configurations for the Built-in Rules.



Rule name: APT 1

Frequency: 45 Minutes

Description: This rule detects APT 1 activity by monitoring tec

☑ Generate Alert

Source index: MITRE ATT&CK

Computer: $.aggregations.Event_group.buckets[*].Computer.buckets[*].key

DSL query

```
{
  "query": {
    "bool": {
      "filter": [
        {
          "bool": {
```

3. After taking the necessary action, click **Save** to update the alert configuration for the selected Built-in rule.

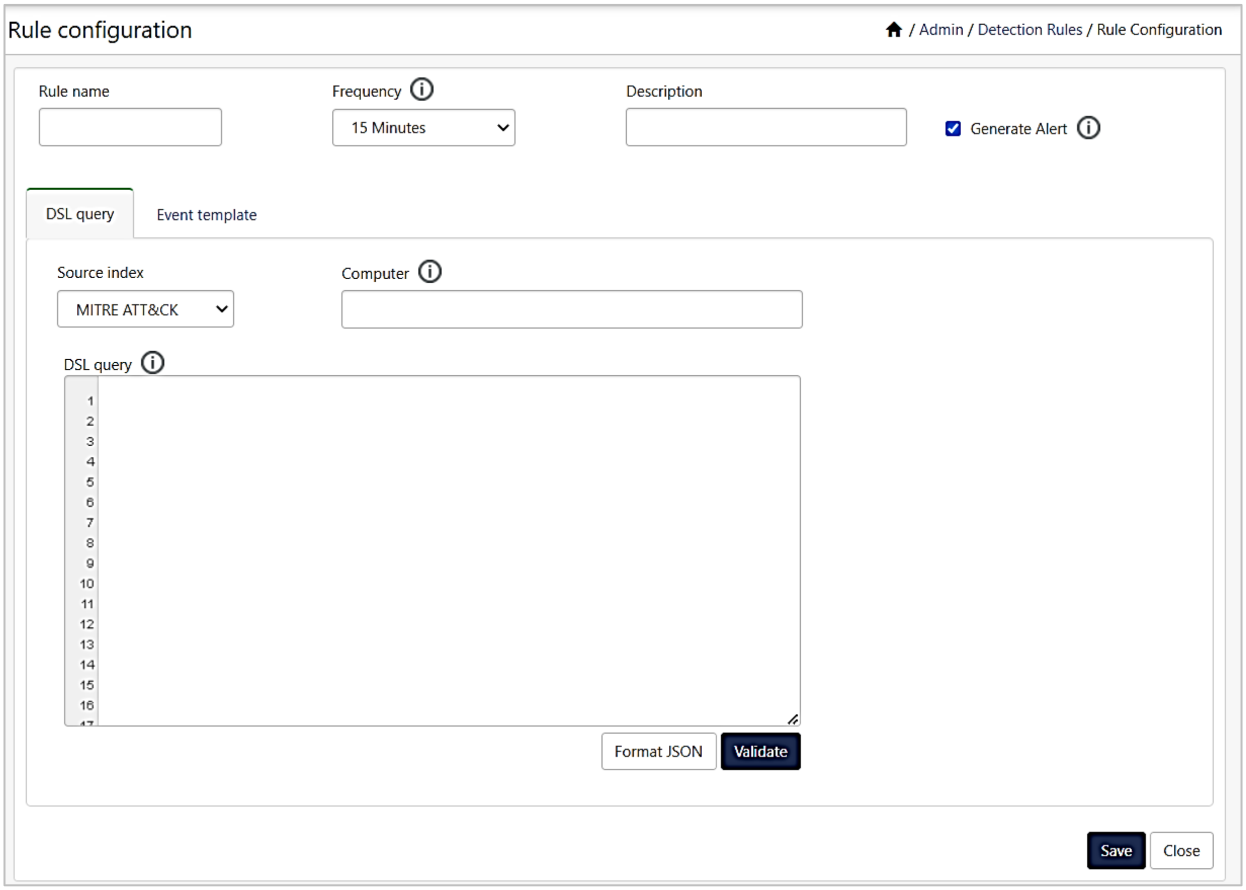
> **Note:**
>
> The event type will be set to WARNING for the triggered event.

## 1.2 Configuring a New Rule

Perform the following procedure to configure a new Rule.

1. In the **Detection Rules** interface, click the **Add Rule** ⊕ button to configure a new rule.

   In the **Rule Configuration** interface, provide the following details to configure the new rule.



Rule configuration

/ Admin / Detection Rules / Rule Configuration

Rule name

Frequency: 15 Minutes

Description

☑ Generate Alert

Source index: MITRE ATT&CK

Computer

DSL query

2. In the **Rule name** field, provide a name for the new Rule Configuration.
3. In the **Frequency** drop-down list, select the recurrence time to execute the Rule according to the selected frequency.
4. In the **Description** field, specify the details of the new rule configuration.

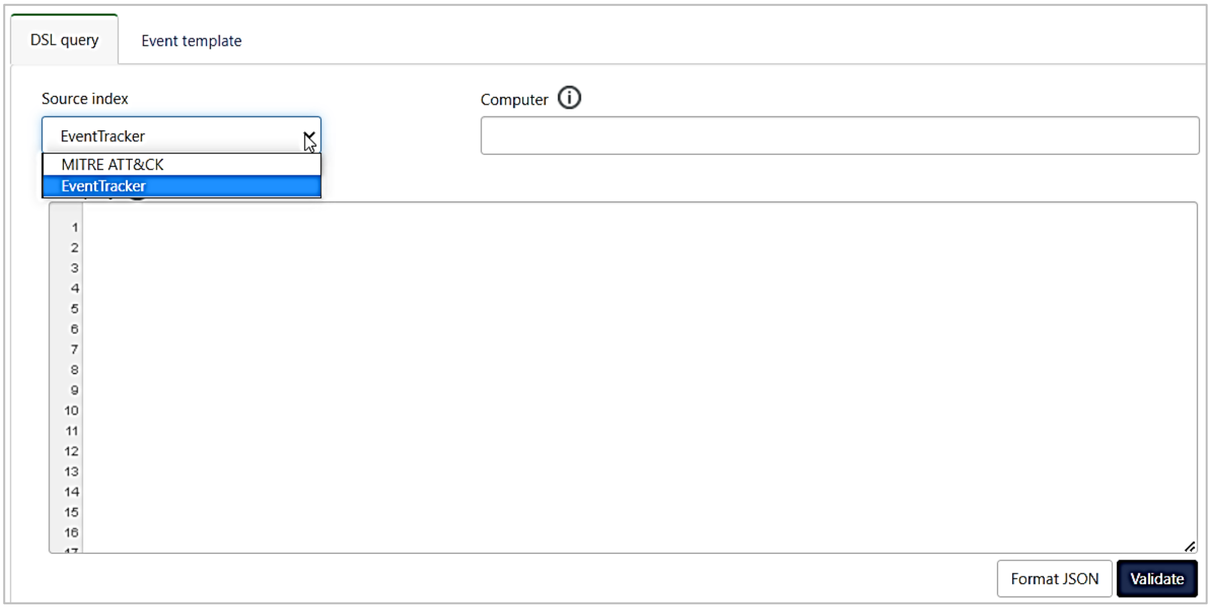
5. Select the **Generate Alert** check box to generate an alert for the new Rule configuration.

> **Note:**
>
> If the **Generate Alert** check box is selected, then, the alert will be triggered upon satisfying the configured rule. But, if the **Generate Alert** check box is not selected, then the alert will not be triggered.

> **Note:**
>
> If the **Generate Alert** check box is selected, then, the alert will be triggered as **EventTracker: Detection rule triggered.**

6. In the **Rules Configuration** interface, click the **DSL query** tab to define the search query.

   - **Source Index:** Select either **MITRE ATT&CK** or **EventTracker** (Elasticsearch) source from the drop-down list to validate and obtain the data.



   - **Computer:** Specify the node path in JSON response using the JSON path syntax, from which the computer name will be extracted and utilized for event generation.
   - **DSL query:** Provide the Bucket aggregation DSL to query and aggregate data based on the selected index and click **Format JSON** to rectify the DSL query in JSON FORMAT.

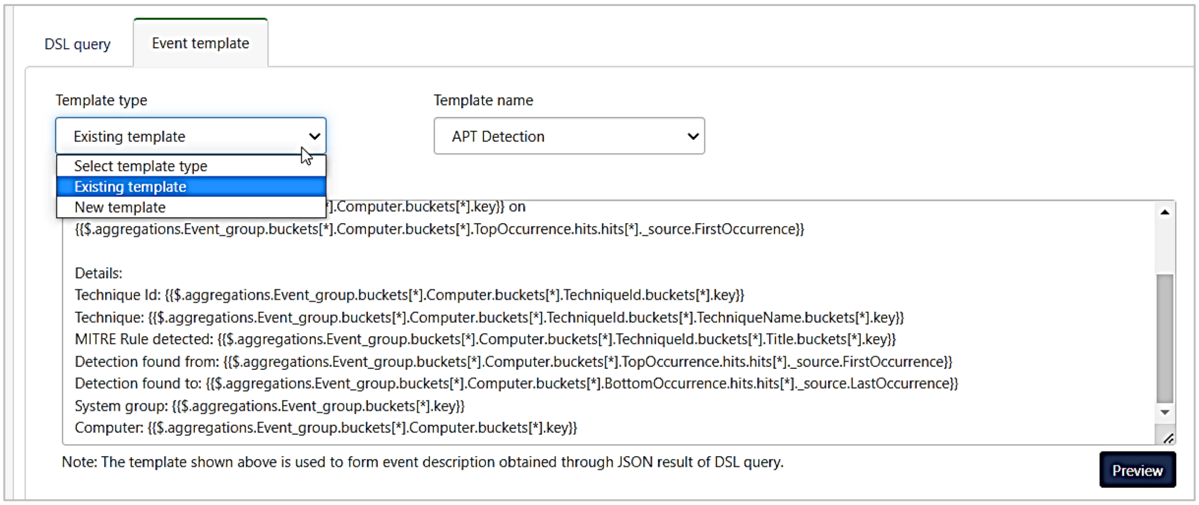
> **Note:**
>
> It is necessary to specify the search area in terms of UTC timeticks, aggregation standards, and the aggregated systems.

   - Click **Format JSON** to rectify the query in JSON format, and after updating the query click **Validate** to verify the DSL query.

7. In the **Rules Configuration** interface, click the **Event template** tab to define the template format for the alert.

   - **Template type**: Select either **Existing template** to use the available template format or **New template** to create the template format from the drop-down list.

**Image Representation for the Existing template**



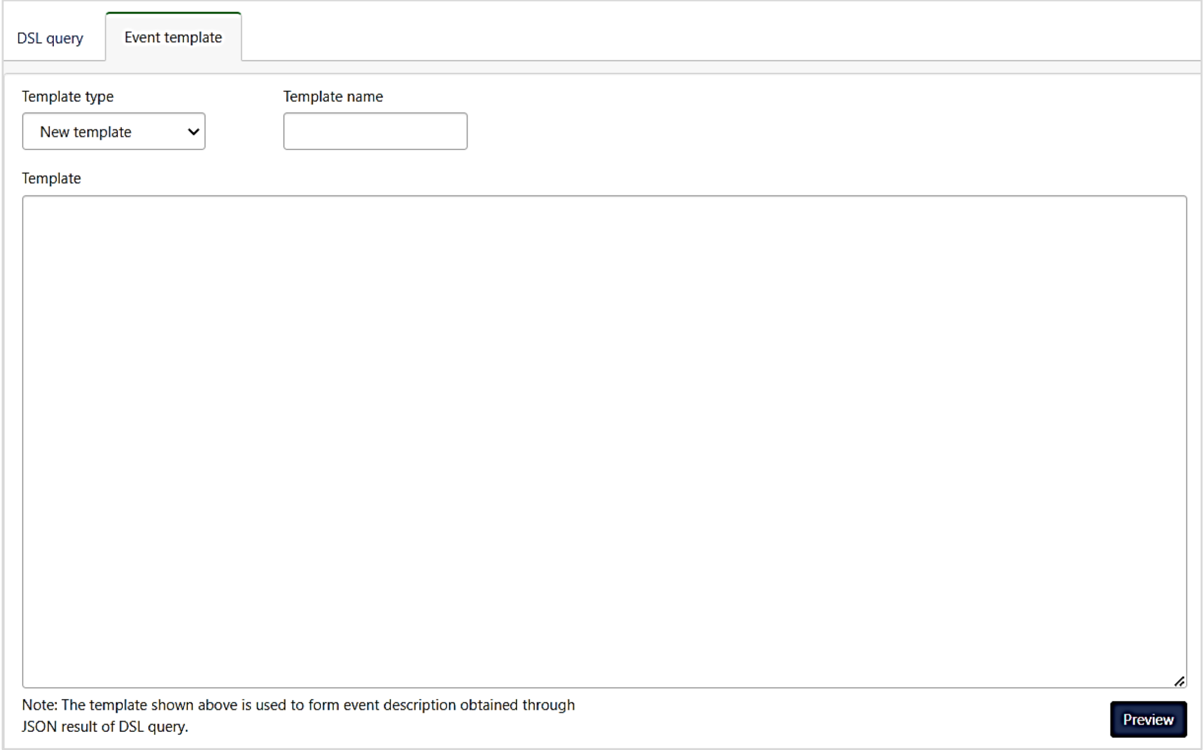
```
]].Computer.buckets[*].key}} on
{{$.aggregations.Event_group.buckets[*].Computer.buckets[*].TopOccurrence.hits.hits[*]._source.FirstOccurrence}}

Details:
Technique Id: {{$.aggregations.Event_group.buckets[*].Computer.buckets[*].TechniqueId.buckets[*].key}}
Technique: {{$.aggregations.Event_group.buckets[*].Computer.buckets[*].TechniqueId.buckets[*].TechniqueName.buckets[*].key}}
MITRE Rule detected: {{$.aggregations.Event_group.buckets[*].Computer.buckets[*].TechniqueId.buckets[*].Title.buckets[*].key}}
Detection found from: {{$.aggregations.Event_group.buckets[*].Computer.buckets[*].TopOccurrence.hits.hits[*]._source.FirstOccurrence}}
Detection found to: {{$.aggregations.Event_group.buckets[*].Computer.buckets[*].BottomOccurrence.hits.hits[*]._source.LastOccurrence}}
System group: {{$.aggregations.Event_group.buckets[*].key}}
Computer: {{$.aggregations.Event_group.buckets[*].Computer.buckets[*].key}}
```

Note: The template shown above is used to form event description obtained through JSON result of DSL query.

| | |
|---|---|
| **Existing template** | If selecting **Existing template**, you can select either the built-in templates (APT Detection, or Brute force, or Password spraying, or Environment Detection, or Environment system detection) or the User-defined templates from the drop-down list that formats event description obtained through JSON result of DSL query.<br>**Note:**<br>You cannot edit the built-in templates but, you can clone a built-in template to a New template. Refer Cloning a Built-in or a User-defined template section for more details.<br>**Note:**<br>You can edit the existing User-defined template. Modifying the existing User-defined template will impact all the rules using that template. Use the **Clone** action if you do not require to reverse the existing User-defined template. |

### Image Representation for the New template



Template type: New template

Template name:

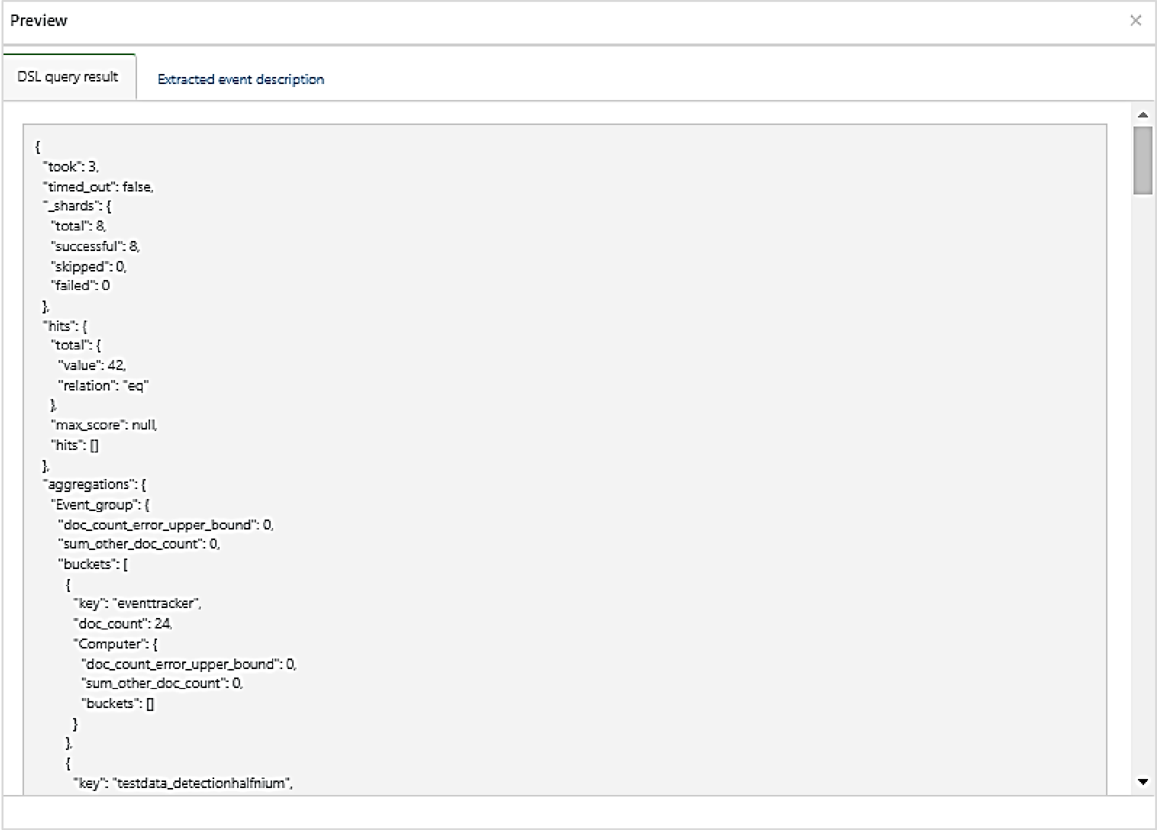
Template

Note: The template shown above is used to form event description obtained through JSON result of DSL query.

| | |
|---|---|
| **New template** | If selecting **New template**, then provide the template name and create a new template format.<br>**Note:**<br>If no rules are associated to a template, then that template will be deleted. |

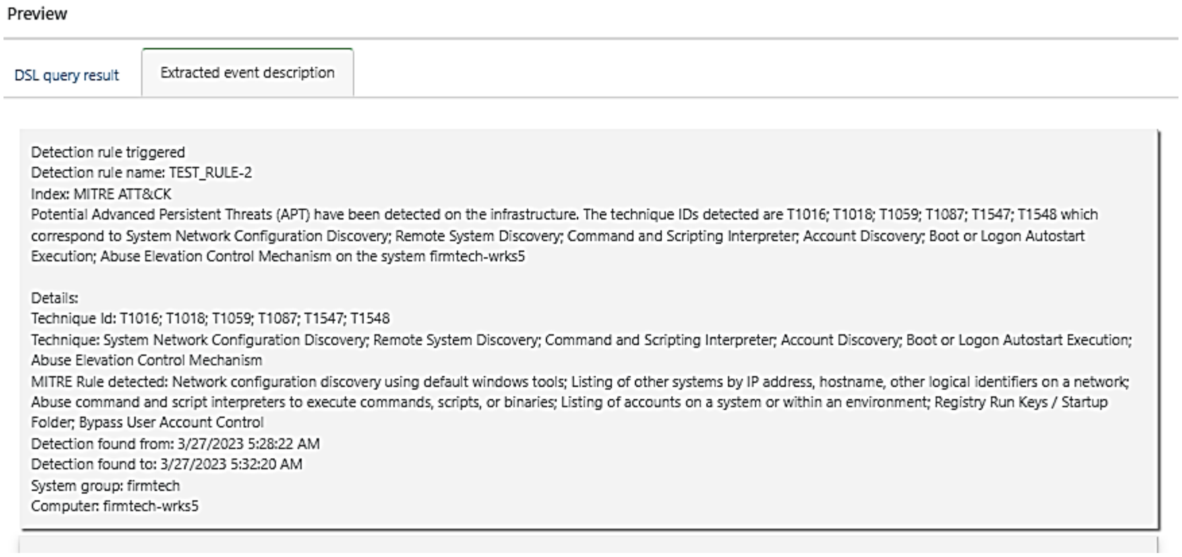
- Click **Preview** to view the **DSL query result** and the **Extracted event description** based on DSL query result.

**DSL query result:**



```
{
  "took": 3,
  "timed_out": false,
  "_shards": {
    "total": 8,
    "successful": 8,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": {
      "value": 42,
      "relation": "eq"
    },
    "max_score": null,
    "hits": []
  },
  "aggregations": {
    "Event_group": {
      "doc_count_error_upper_bound": 0,
      "sum_other_doc_count": 0,
      "buckets": [
        {
          "key": "eventtracker",
          "doc_count": 24,
          "Computer": {
            "doc_count_error_upper_bound": 0,
            "sum_other_doc_count": 0,
            "buckets": []
          }
        },
        {
          "key": "testdata_detectionhalfnium",
```

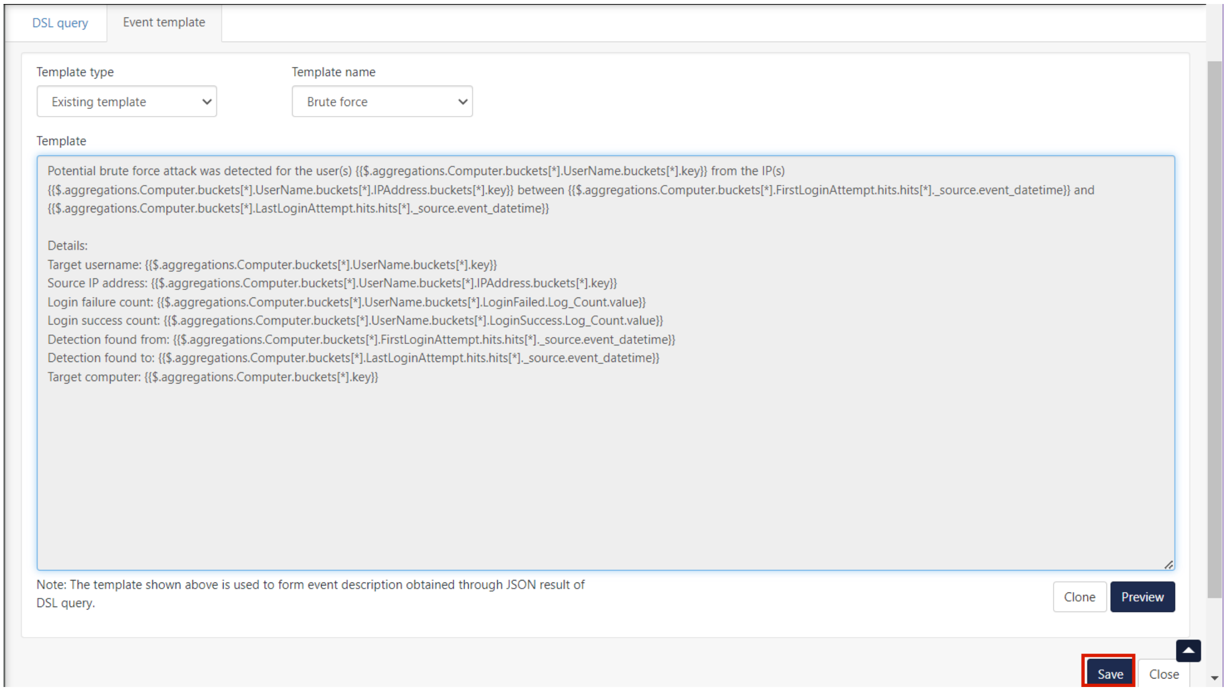
**Extracted event description:**



Detection rule triggered
Detection rule name: TEST_RULE-2
Index: MITRE ATT&CK
Potential Advanced Persistent Threats (APT) have been detected on the infrastructure. The technique IDs detected are T1016; T1018; T1059; T1087; T1547; T1548 which correspond to System Network Configuration Discovery; Remote System Discovery; Command and Scripting Interpreter; Account Discovery; Boot or Logon Autostart Execution; Abuse Elevation Control Mechanism on the system firmtech-wrks5

Details:
Technique Id: T1016; T1018; T1059; T1087; T1547; T1548
Technique: System Network Configuration Discovery; Remote System Discovery; Command and Scripting Interpreter; Account Discovery; Boot or Logon Autostart Execution; Abuse Elevation Control Mechanism
MITRE Rule detected: Network configuration discovery using default windows tools; Listing of other systems by IP address, hostname, other logical identifiers on a network; Abuse command and script interpreters to execute commands, scripts, or binaries; Listing of accounts on a system or within an environment; Registry Run Keys / Startup Folder; Bypass User Account Control
Detection found from: 3/27/2023 5:28:22 AM
Detection found to: 3/27/2023 5:32:20 AM
System group: firmtech
Computer: firmtech-wrks5

8. After providing all the details, click **Save** to save the newly created Rule configuration.



Template type: Existing template

Template name: Brute force

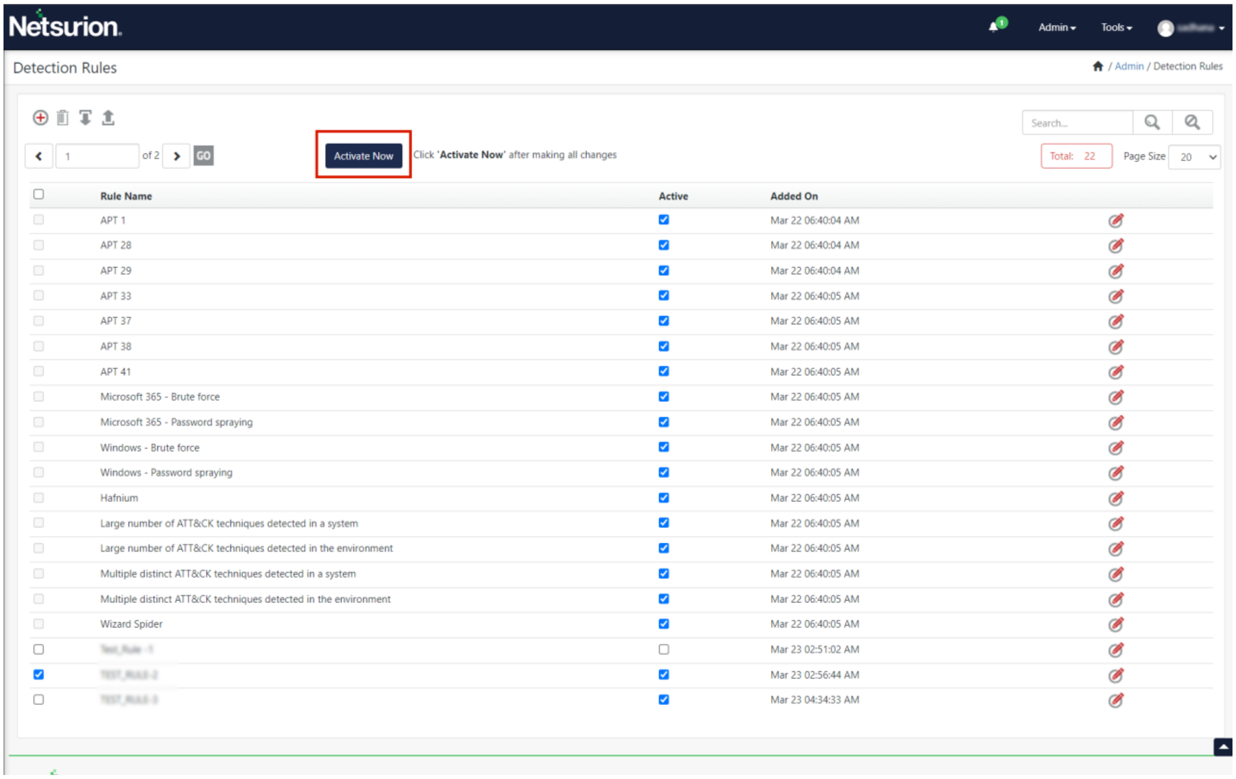
Template

Potential brute force attack was detected for the user(s) {{$.aggregations.Computer.buckets[*].UserName.buckets[*].key}} from the IP(s) {{$.aggregations.Computer.buckets[*].UserName.buckets[*].IPAddress.buckets[*].key}} between {{$.aggregations.Computer.buckets[*].FirstLoginAttempt.hits.hits[*]._source.event_datetime}} and {{$.aggregations.Computer.buckets[*].LastLoginAttempt.hits.hits[*]._source.event_datetime}}

Details:
Target username: {{$.aggregations.Computer.buckets[*].UserName.buckets[*].key}}
Source IP address: {{$.aggregations.Computer.buckets[*].UserName.buckets[*].IPAddress.buckets[*].key}}
Login failure count: {{$.aggregations.Computer.buckets[*].UserName.buckets[*].LoginFailed.Log_Count.value}}
Login success count: {{$.aggregations.Computer.buckets[*].UserName.buckets[*].LoginSuccess.Log_Count.value}}
Detection found from: {{$.aggregations.Computer.buckets[*].FirstLoginAttempt.hits.hits[*]._source.event_datetime}}
Detection found to: {{$.aggregations.Computer.buckets[*].LastLoginAttempt.hits.hits[*]._source.event_datetime}}
Target computer: {{$.aggregations.Computer.buckets[*].key}}

Note: The template shown above is used to form event description obtained through JSON result of DSL query.

9. Then, go to the **Detection Rules** interface, click **Activate Now** to activate the newly added Detection Rule.



Click '**Activate Now**' after making all changes

Total: 22 Page Size 20

| ☐ | Rule Name | Active | Added On |
|---|---|---|---|
| ☐ | APT 1 | ☑ | Mar 22 06:40:04 AM |
| ☐ | APT 28 | ☑ | Mar 22 06:40:04 AM |
| ☐ | APT 29 | ☑ | Mar 22 06:40:04 AM |
| ☐ | APT 33 | ☑ | Mar 22 06:40:05 AM |
| ☐ | APT 37 | ☑ | Mar 22 06:40:05 AM |
| ☐ | APT 38 | ☑ | Mar 22 06:40:05 AM |
| ☐ | APT 41 | ☑ | Mar 22 06:40:05 AM |
| ☐ | Microsoft 365 - Brute force | ☑ | Mar 22 06:40:05 AM |
| ☐ | Microsoft 365 - Password spraying | ☑ | Mar 22 06:40:05 AM |
| ☐ | Windows - Brute force | ☑ | Mar 22 06:40:05 AM |
| ☐ | Windows - Password spraying | ☑ | Mar 22 06:40:05 AM |
| ☐ | Hafnium | ☑ | Mar 22 06:40:05 AM |
| ☐ | Large number of ATT&CK techniques detected in a system | ☑ | Mar 22 06:40:05 AM |
| ☐ | Large number of ATT&CK techniques detected in the environment | ☑ | Mar 22 06:40:05 AM |
| ☐ | Multiple distinct ATT&CK techniques detected in a system | ☑ | Mar 22 06:40:05 AM |
| ☐ | Multiple distinct ATT&CK techniques detected in the environment | ☑ | Mar 22 06:40:05 AM |
| ☐ | Wizard Spider | ☑ | Mar 22 06:40:05 AM |
| ☐ | [redacted] | ☐ | Mar 23 02:51:02 AM |
| ☑ | [redacted] | ☑ | Mar 23 02:56:44 AM |
| ☐ | [redacted] | ☑ | Mar 23 04:34:33 AM |

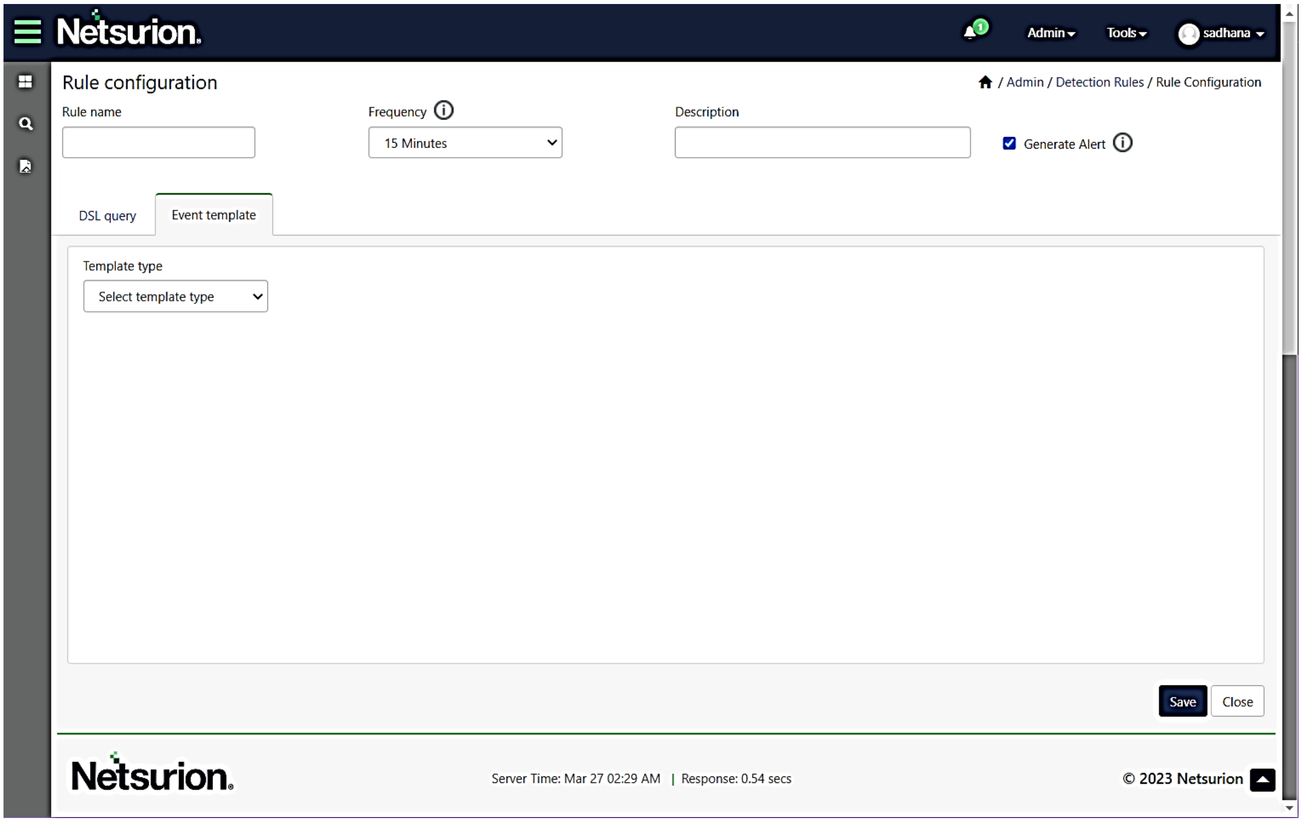
## 1.3 Cloning a Built-in or a User-defined template

The Open XDR platform facilitates to modify and reutilize the Built-in or the existing User-defined templates. The cloning feature supports creating new templates including the details of the existing Built-in or the User-defined template.

Perform the following procedure to clone a Built-in template.

1. In the new **Rule Configuration** interface, after the providing the necessary details for the Rule name, Frequency, and DSL query, go to the **Event template** tab.

> **Note:**
>
> Refer Configuring a New Rule section to view the detailed process for configuring a new rule.



Rule configuration

Rule name:

Frequency: 15 Minutes

Description:

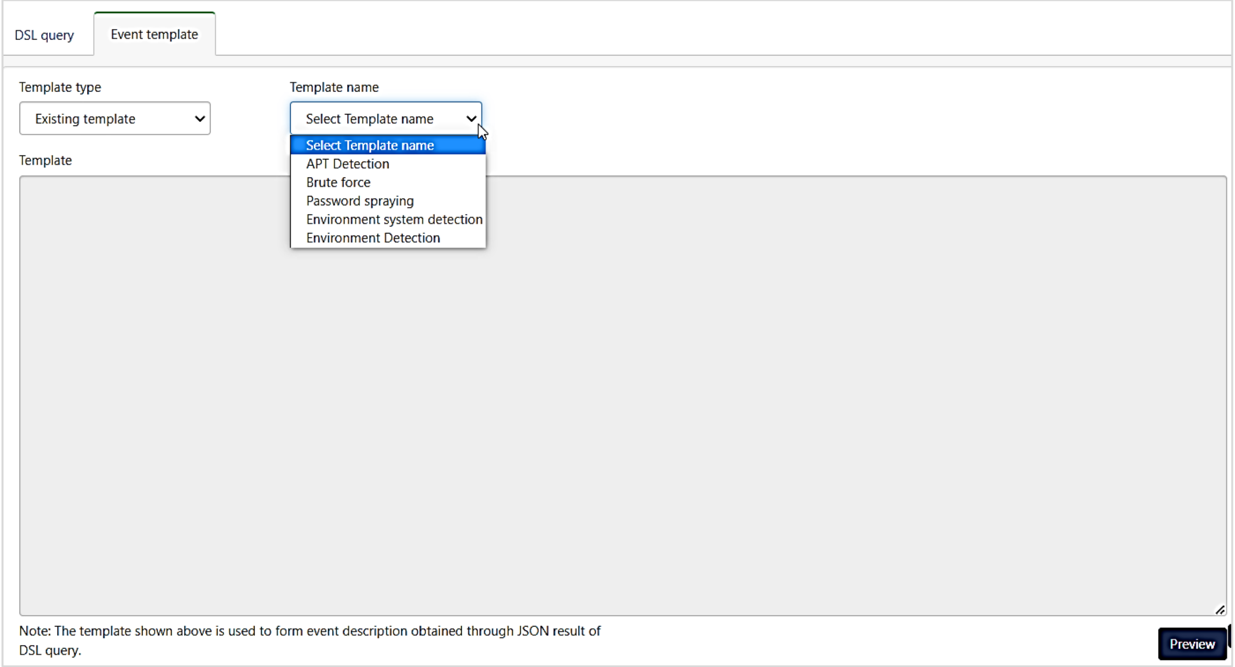
☑ Generate Alert

Template type: Select template type

Server Time: Mar 27 02:29 AM | Response: 0.54 secs

© 2023 Netsurion

2. In the **Event template** tab, select the Template type as **Existing template** and select the appropriate existing Built-in **Template name** from the drop-down list.



Template type: Existing template

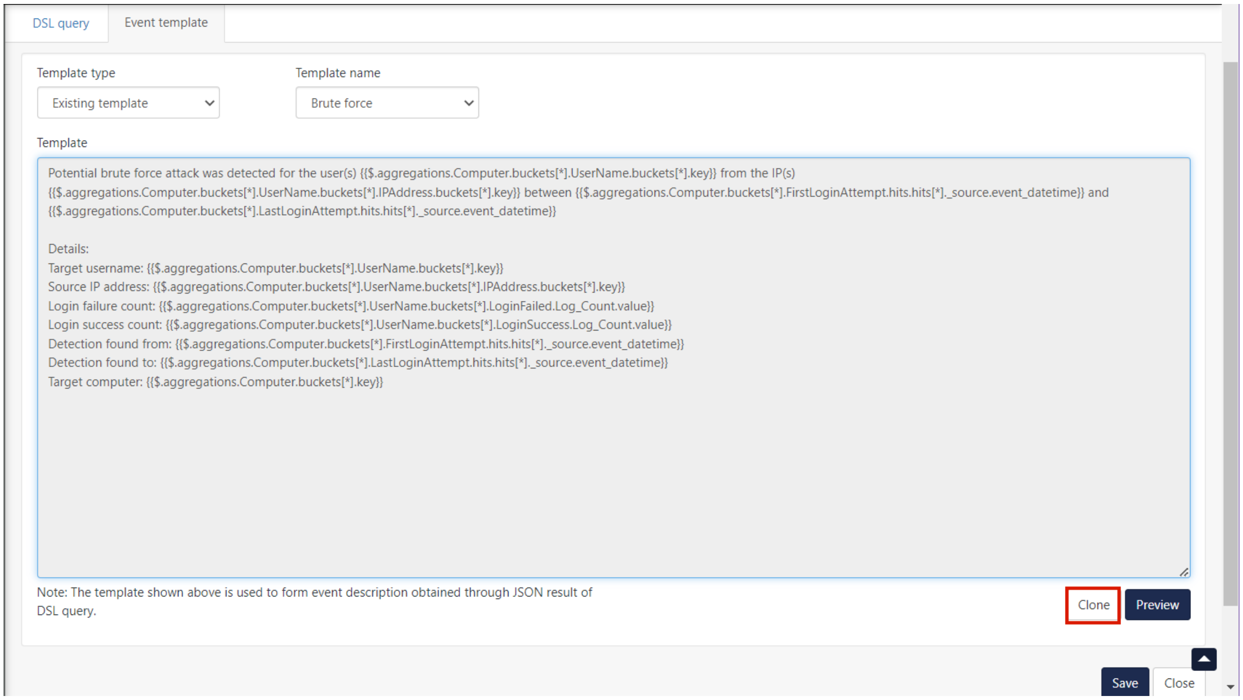
Template name: Select Template name

Template

Note: The template shown above is used to form event description obtained through JSON result of DSL query.

When the necessary Built-in template is chosen, the **Clone** action button appears in the bottom right-corner of the interface.

3. Click **Clone** to create a user-defined template with the details of the selected Existing template.



Template type: Existing template

Template name: Brute force

Template

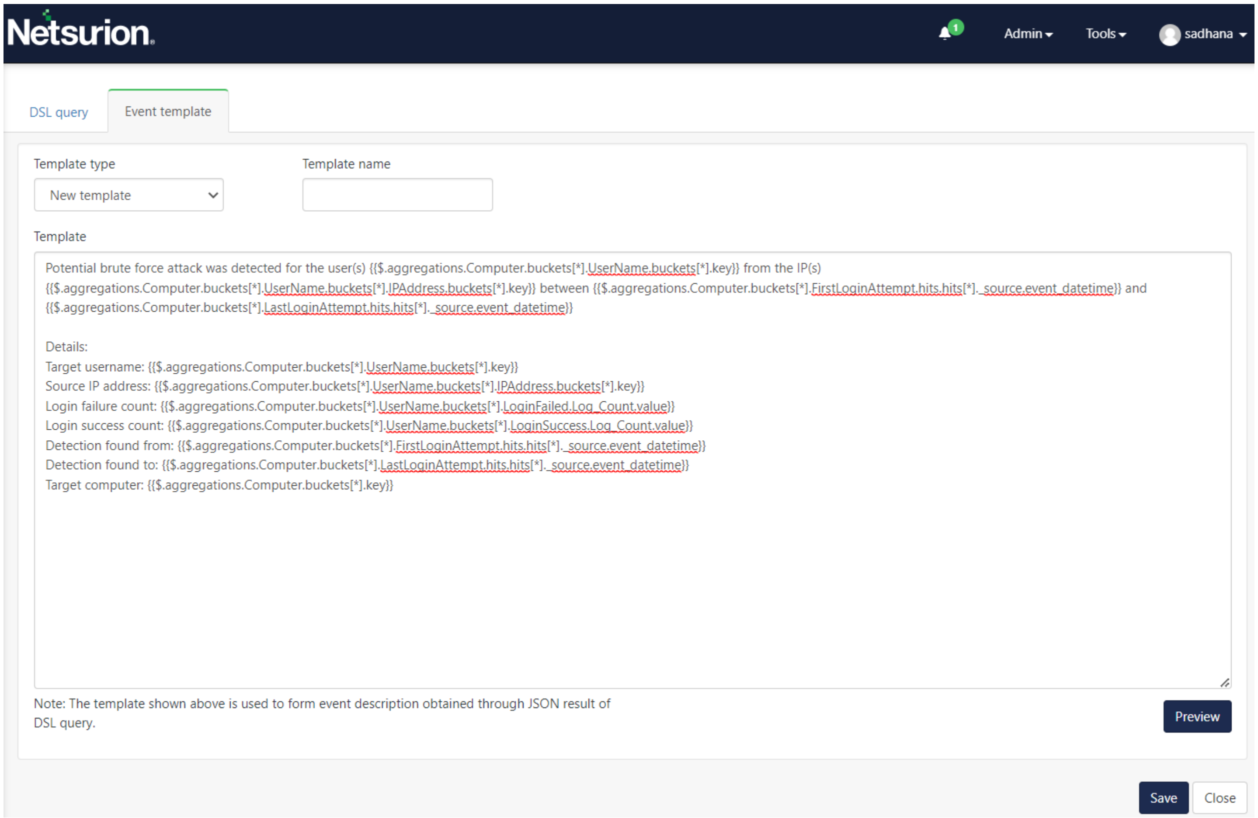
```
Potential brute force attack was detected for the user(s) {{$.aggregations.Computer.buckets[*].UserName.buckets[*].key}} from the IP(s)
{{$.aggregations.Computer.buckets[*].UserName.buckets[*].IPAddress.buckets[*].key}} between {{$.aggregations.Computer.buckets[*].FirstLoginAttempt.hits.hits[*]._source.event_datetime}} and
{{$.aggregations.Computer.buckets[*].LastLoginAttempt.hits.hits[*]._source.event_datetime}}

Details:
Target username: {{$.aggregations.Computer.buckets[*].UserName.buckets[*].key}}
Source IP address: {{$.aggregations.Computer.buckets[*].UserName.buckets[*].IPAddress.buckets[*].key}}
Login failure count: {{$.aggregations.Computer.buckets[*].UserName.buckets[*].LoginFailed.Log_Count.value}}
Login success count: {{$.aggregations.Computer.buckets[*].UserName.buckets[*].LoginSuccess.Log_Count.value}}
Detection found from: {{$.aggregations.Computer.buckets[*].FirstLoginAttempt.hits.hits[*]._source.event_datetime}}
Detection found to: {{$.aggregations.Computer.buckets[*].LastLoginAttempt.hits.hits[*]._source.event_datetime}}
Target computer: {{$.aggregations.Computer.buckets[*].key}}
```

Note: The template shown above is used to form event description obtained through JSON result of DSL query.

The DSL query of the Existing template will be replicated to the New template and you can make the necessary modifications.

4. Provide a unique Template name and after making the modifications click **Save** to save the new template format.



Template type: New template

Template name:

Template

```
Potential brute force attack was detected for the user(s) {{$.aggregations.Computer.buckets[*].UserName.buckets[*].key}} from the IP(s)
{{$.aggregations.Computer.buckets[*].UserName.buckets[*].IPAddress.buckets[*].key}} between {{$.aggregations.Computer.buckets[*].FirstLoginAttempt.hits.hits[*]._source.event_datetime}} and
{{$.aggregations.Computer.buckets[*].LastLoginAttempt.hits.hits[*]._source.event_datetime}}

Details:
Target username: {{$.aggregations.Computer.buckets[*].UserName.buckets[*].key}}
Source IP address: {{$.aggregations.Computer.buckets[*].UserName.buckets[*].IPAddress.buckets[*].key}}
Login failure count: {{$.aggregations.Computer.buckets[*].UserName.buckets[*].LoginFailed.Log_Count.value}}
Login success count: {{$.aggregations.Computer.buckets[*].UserName.buckets[*].LoginSuccess.Log_Count.value}}
Detection found from: {{$.aggregations.Computer.buckets[*].FirstLoginAttempt.hits.hits[*]._source.event_datetime}}
Detection found to: {{$.aggregations.Computer.buckets[*].LastLoginAttempt.hits.hits[*]._source.event_datetime}}
Target computer: {{$.aggregations.Computer.buckets[*].key}}
```

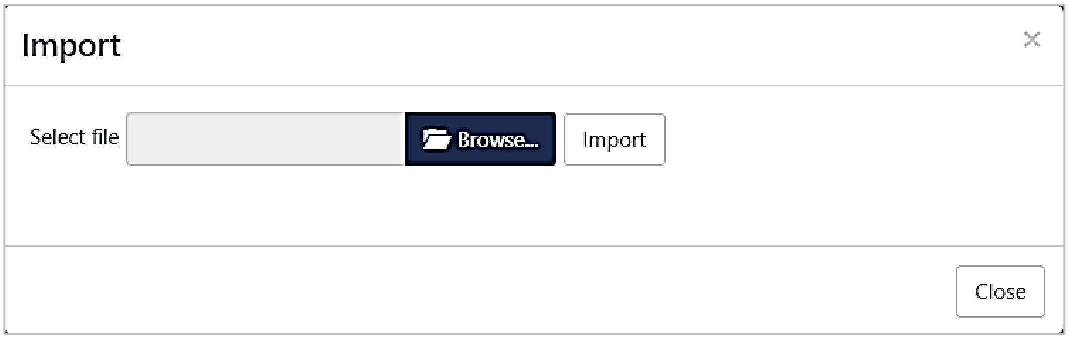
Note: The template shown above is used to form event description obtained through JSON result of DSL query.

5. Then, go to the **Detection Rules** interface, select the newly cloned rule name check box from the Rule list and click **Activate Now** to activate the Rule.

## 1.4 Importing a Rule Configuration

Perform the following procedure to import a Rule Configuration.

1. In the **Detection Rules** interface, click the **Import** ⭳ button to import the Rule configuration.
2. In the **Import** window, click **Browse** to select the **.etdr** file and then click **Import** to import the file details.

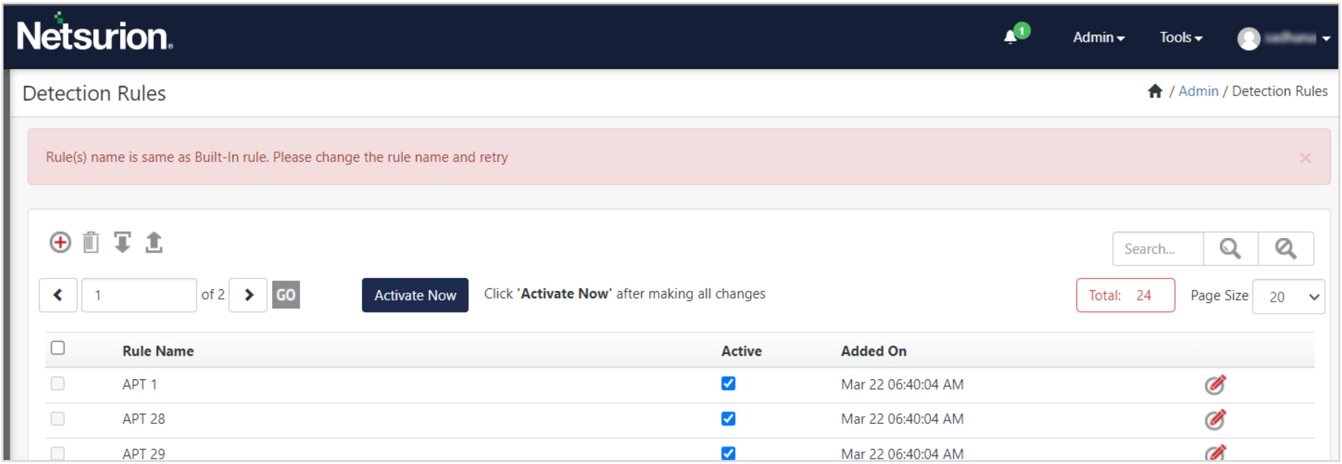


## Importing a Rule with Built-in Rule Name

**Note:**

You cannot import a Rule with the Built-in Rule name.

The following error message stating ‘***Rule(s) name is same as Built-in rule. Please change the rule name and retry.***’ appears if you try to import a Rule with the Built-in Rule name.



Rule(s) name is same as Built-In rule. Please change the rule name and retry

1 of 2

Click '**Activate Now**' after making all changes

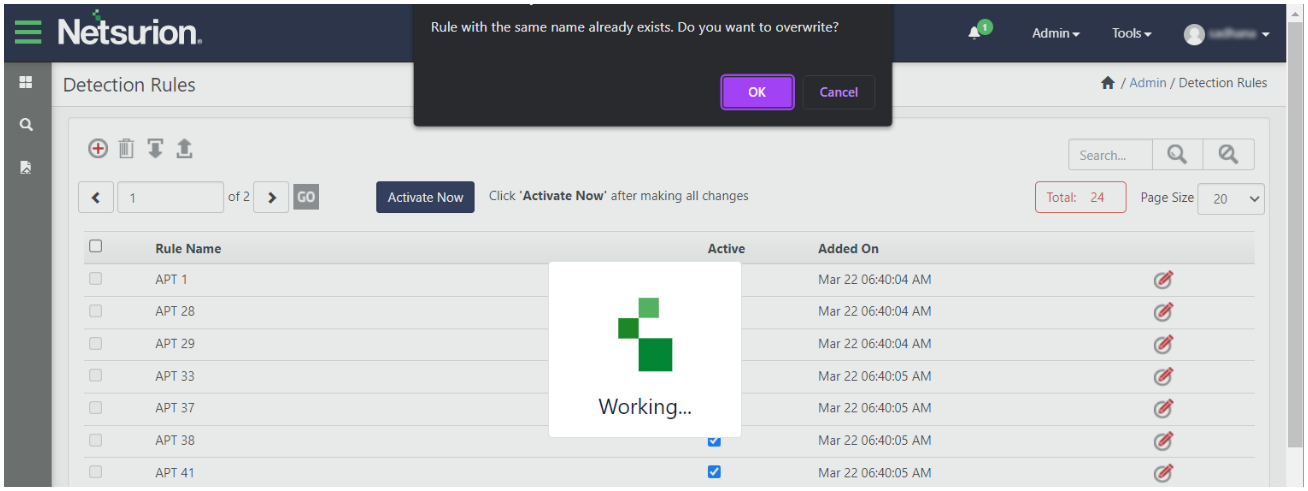
Total: 24

| □ | Rule Name | Active | Added On |
|---|---|---|---|
| □ | APT 1 | ☑ | Mar 22 06:40:04 AM |
| □ | APT 28 | ☑ | Mar 22 06:40:04 AM |
| □ | APT 29 | ☑ | Mar 22 06:40:04 AM |

## Importing a Rule with Existing Rule Name

Importing a rule with existing rule name will overwrite the configurations of the existing rule. The following confirmation message stating ‘***Rule with same name already exists. Do you want to overwrite?***’ appears.

- Click **OK** to overwrite or **Cancel** to terminate the process.



Rule with the same name already exists. Do you want to overwrite?

1 of 2

Click '**Activate Now**' after making all changes

Total: 24

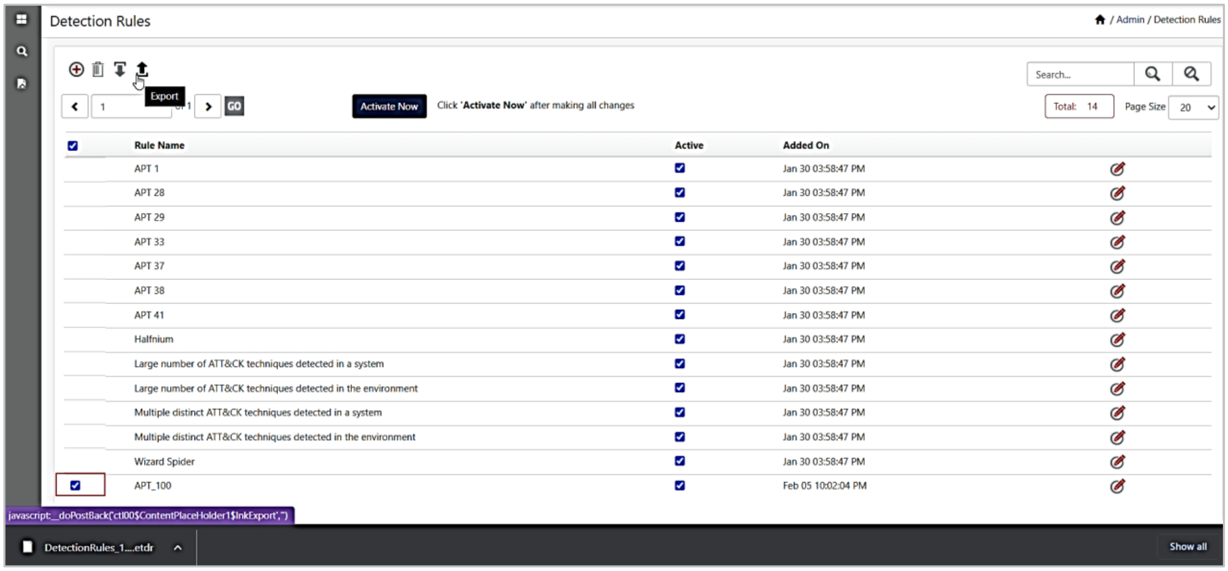
| □ | Rule Name | Active | Added On |
|---|---|---|---|
| □ | APT 1 | | Mar 22 06:40:04 AM |
| □ | APT 28 | | Mar 22 06:40:04 AM |
| □ | APT 29 | | Mar 22 06:40:04 AM |
| □ | APT 33 | | Mar 22 06:40:05 AM |
| □ | APT 37 | | Mar 22 06:40:05 AM |
| □ | APT 38 | ☑ | Mar 22 06:40:05 AM |
| □ | APT 41 | ☑ | Mar 22 06:40:05 AM |

## 1.5 Exporting a Rule Configuration

Perform the following procedure to export a Rule Configuration.

- In the **Detection Rules** interface, select the required Detection Rules from the list and then click the **Export** button to export the configured rules.

> **Note:**
>
> The default Rules (that is, the Built-in rules) cannot be exported.



Click **'Activate Now'** after making all changes

| ☑ | Rule Name | Active | Added On | |
|---|---|---|---|---|
| | APT 1 | ☑ | Jan 30 03:58:47 PM | |
| | APT 28 | ☑ | Jan 30 03:58:47 PM | |
| | APT 29 | ☑ | Jan 30 03:58:47 PM | |
| | APT 33 | ☑ | Jan 30 03:58:47 PM | |
| | APT 37 | ☑ | Jan 30 03:58:47 PM | |
| | APT 38 | ☑ | Jan 30 03:58:47 PM | |
| | APT 41 | ☑ | Jan 30 03:58:47 PM | |
| | Halfnium | ☑ | Jan 30 03:58:47 PM | |
| | Large number of ATT&CK techniques detected in a system | ☑ | Jan 30 03:58:47 PM | |
| | Large number of ATT&CK techniques detected in the environment | ☑ | Jan 30 03:58:47 PM | |
| | Multiple distinct ATT&CK techniques detected in a system | ☑ | Jan 30 03:58:47 PM | |
| | Multiple distinct ATT&CK techniques detected in the environment | ☑ | Jan 30 03:58:47 PM | |
| | Wizard Spider | ☑ | Jan 30 03:58:47 PM | |
| ☑ | APT_100 | ☑ | Feb 05 10:02:04 PM | |

javascript:__doPostBack('ctl00$ContentPlaceHolder1$lnkExport','')

## About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's Managed Threat Protection includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at www.netsurion.com.

## Contact Us

### Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

### Contact Numbers

| | | |
|---|---|---|
| Direct Enterprise | SOC@Netsurion.com | 1 (877) 333-1433 Option 1, Option 1 |
| MSP Enterprise | SOC-MSP@Netsurion.com | 1 (877) 333-1433 Option 1, Option 2 |
| Essentials | Essentials-Support@Netsurion.com | 1 (877) 333-1433 Option 1, Option 3 |
| Self-Serve | EventTracker-Support@Netsurion.com | 1 (877) 333-1433 Option 1, Option 4 |

https://www.netsurion.com/eventtracker-support