



## Feature Guide

# Event Correlator

### Publication Date

March 06, 2024

## Abstract

This document provides the features of the Event Correlator, steps to create correlation rules, and generate relevant reports.

**Note:**

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

## Scope

The Configuration details in this guide are consistent with Netsurion Open XDR 9.4.

## Audience

This guide is for the administrators responsible for managing Event Correlator.

## Table of Contents

<b>1</b>	<b>Overview</b>	<b>4</b>
1.1	Role of Event Correlation Rules in Netsurion Open XDR	4
<b>2</b>	<b>Netsurion Open XDR Correlator</b>	<b>5</b>
2.1	Real-time Correlator	5
2.2	On-Demand Correlator	5
<b>3</b>	<b>Prerequisites</b>	<b>5</b>
<b>4</b>	<b>Configure Correlation Rules</b>	<b>6</b>
4.1	To Create a New Correlation Rule	6
4.2	Action Item to Run a Script	13
4.3	To Edit a Correlation Rule	15
4.4	To Delete a Correlation Rule	17
<b>5</b>	<b>Generate Netsurion Open XDR Correlation Events Report</b>	<b>18</b>
5.1	Configure Reports	18
<b>6</b>	<b>Examples</b>	<b>20</b>
6.1	Correlation of Two Events	20
6.2	Search for a Particular Substring	21
6.3	Add Event Properties Description in the Action Event	22
6.3.1	In the Presence of Event Source Description	22
6.3.2	In the Absence of Event Source Description	23
<b>7</b>	<b>Steps to Enable Group-Level Event Correlation</b>	<b>25</b>

# 1 Overview

Netsurion Open XDR Correlator is a feature add-on package, which runs along with Netsurion Open XDR. It compares and matches the pattern of predefined events to identify the correlation conditions. Correlation is a class of statistical relationships between two or more variables or observed data values.

It is the process of analyzing events to identify patterns. This helps pinpoint problems such as abuse, intrusion, attacks, or failure.

## 1.1 Role of Event Correlation Rules in Netsurion Open XDR

Netsurion Open XDR uses correlation rules to keep track of enterprise network behavior and its entities. This helps an organization to determine the possible states and generate appropriate action events. Here, the correlation rules relate the incoming events and generate the alert based on the predefined rule details, if Netsurion Open XDR real-time Correlator is installed.

The rules are governed by business logic and a well-defined format which will be deciphered by the 'Correlation engine'. Each correlation rule will be a named rule and each rule must define at least one event and one action event against that event. The Events and Action events are in N > N relation, provided each rule set adheres to the following constraints.

### Constraints for Event:

- Each event must have a label and must be unique to that correlation rule.
- No events can be repeated within that correlation rule.
- At least one event rule must be defined.
- Period and occurrence both must be specified.
- Can have a back reference to the preceding event as the placeholder for data within the same rule.

### Constraints for Event Actions (If Netsurion Open XDR real-time Correlator is installed):

- Each action event must have a label and must be unique to that correlation rule.
- No action event can be repeated within that correlation rule.
- At least one 'Action event rule' must be defined.
- An action event can be constructed by referring to any of the previous events generated.

### Note

Correlation can work in real-time (online) as well as on-demand (offline). However, action events will only work online, that is only if Netsurion Open XDR real-time Correlator is installed.

## 2 Netsurion Open XDR Correlator

Netsurion Open XDR's correlation engine is divided into two parts, a Real-time Correlator and an On-demand Correlator.

### 2.1 Real-time Correlator

It correlates the received events from the agent and performs the action based on the specified rule. The real-time correlator engine processes the event as it comes and generates new events according to the specified behavior pattern. The correlation rule will take place only when the events show the defined pattern of occurrence. A set of predefined alerts are available by default and these alerts can be activated as per the requirement.

### 2.2 On-Demand Correlator

The selected correlation rule will be applied while processing the on-demand report. The report will be generated based on the properties given in the source event. The action event properties will not be considered while generating the report. If the generated events pass through the correlator rule parser, then the generated report will contain information on all the events that occurred within the given lifetime.

## 3 Prerequisites

- Netsurion Open XDR 9.4 must be installed, and the customer should have a license for the Real-time and On-Demand features respectively.
- Netsurion Open XDR Correlator update must be applied to the Netsurion Open XDR Console. You can access the same from [here](#).

#### Note

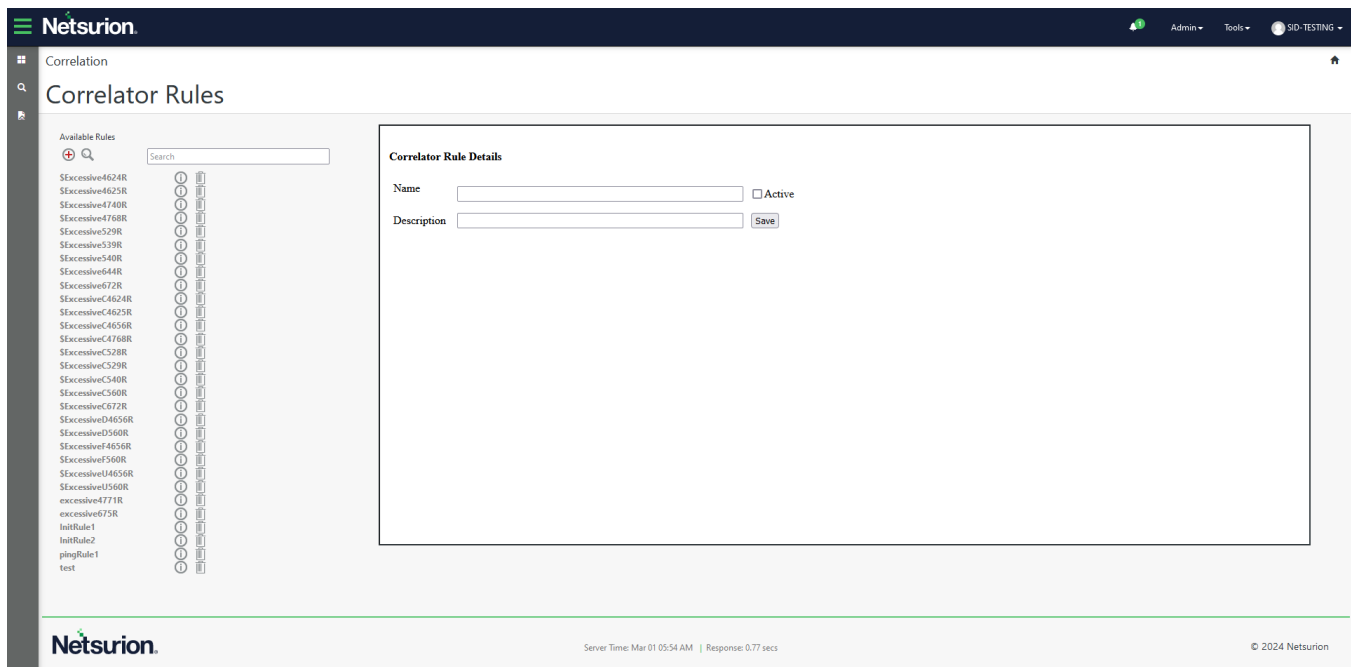
During the upgrade, the user must re-apply the respective feature add-on for the respective version of Netsurion Open XDR installed. Later, the user must traverse to Admin, select any existing rule, and save it to make sure that custom alerts and reports are retained.

## 4 Configure Correlation Rules

By default, Netsurion Open XDR has activated some correlation rules in the default rule base. The default rule base contains the predefined correlation rules and an option to add a new correlation rule.

### 4.1 To Create a New Correlation Rule

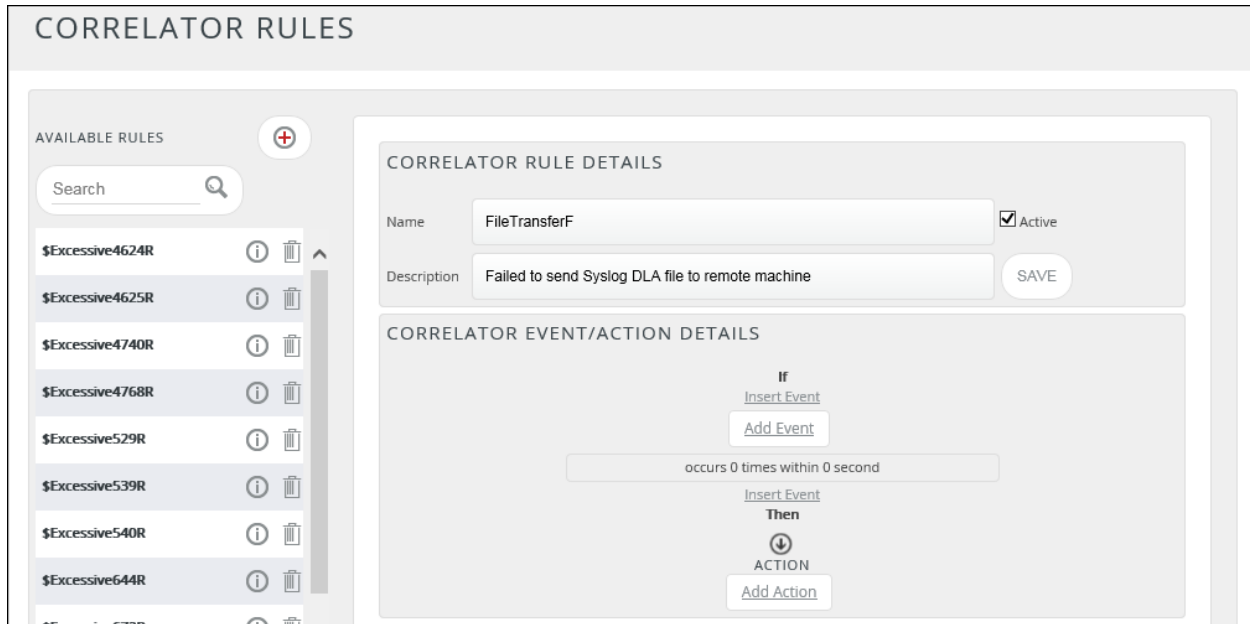
1. Log in to Netsurion Open XDR.
2. Click the **Admin** dropdown, and then select **Correlation**. The **Correlator Rules** page will be displayed as shown below:



3. The left pane displays the list of correlation rules available, and the right pane displays a page to add new correlation rules or edit the selected rule details.
4. In the **Correlator Rule Details** pane, enter the rule name in the **Name** field.

Example: File Transfer

- This rule name will be unique across the Correlator Rules.
  - The input field should not contain space or special characters.
5. Enter the description for the rule in the description field. Example: Failed to send Syslog DLA file to the remote machine.
  6. Select the **Active** checkbox to activate the rule. If you do not select the Active checkbox, then the Correlation rule will only get saved and will not be activated.
  7. Click **Save**. Netsurion Open XDR displays the Correlator event/Action Details pane.



8. Click the **Add Event** hyperlink. The Properties dialog box will be displayed as shown below:

Internet Explorer - Properties

### EVENT PROPERTIES

Label\*

Life Time (seconds)\*

Occurrence\*

Log Type  ▼

Event Type  ▼

Category

Source

Event Id

User

Computer

Domain

Description

Look for substring
  Look for substring sequence
  Substring and numeric patterns

ADD CANCEL

Executable File	Description
<b>Label</b>	A name given to the Event/Event Action. It is unique across a correlation rule. *This is a mandatory field.
<b>Lifetime (seconds)</b>	Specify the time limit (in seconds) of the event to hold for correlation. *This is a mandatory field.



<b>Occurrence</b>	<p>Enter the number of occurrences of the event to be monitored within a specified duration.</p> <p>*This is a mandatory field.</p>
<b>Log Type</b>	<p>Log type of the event. (1=System, 2=Security, 3=Application)</p>
<b>Event Type</b>	<p>Event type. (1= Error, 2=Warning, 3=Info, 4=Audit Success, 5=Audit Failure)</p>
<b>Category</b>	<p>Enter the event category.</p>
<b>Source</b>	<p>Enter the source of events.</p>
<b>Event ID</b>	<p>Enter the Event ID if you wish to collect the event for the Event ID.</p>
<b>User</b>	<p>Enter the username if you wish to monitor the events for the user.</p>
<b>Computer</b>	<p>Enter the system name if you wish to collect the events from the system.</p>
<b>Domain</b>	<p>Enter the domain name.</p>
<b>Description</b>	<ul style="list-style-type: none"> <li> <b>Select Look for substring:</b> <div data-bbox="500 1098 1393 1291" style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <p>Description</p> <p> <input checked="" type="radio"/> Look for substring           <input type="radio"/> Look for substring sequence           <input type="radio"/> Substring and numeric patterns         </p> <div style="border: 1px solid gray; height: 20px; width: 100%;"></div> </div> <p>Enter the event details to be searched for in the event description field.</p> <p>An Event will be generated only if the event description matches the given criteria.</p> </li> <li> <b>Select Look for substring sequences:</b> <div data-bbox="500 1486 1393 1638" style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <p>Description</p> <p> <input type="radio"/> Look for substring           <input checked="" type="radio"/> Look for substring sequence           <input type="radio"/> Substring and numeric patterns         </p> <div style="display: flex; align-items: center;"> <div style="border: 1px solid gray; flex-grow: 1; height: 20px;"></div> <span style="margin: 0 5px;">Followed by</span> <div style="border: 1px solid gray; flex-grow: 1; height: 20px;"></div> </div> </div> <p>Enter the search criteria in the sequence.</p> <p>For example: 'Manager 192.168.1.4' Followed by 'Status Failed'.</p> <p>An Event will be generated only if the event description matches the given sequence.</p> </li> </ul>

- **Select Substrings and Numeric Patterns:**

Description

Look for substring
  Look for substring sequence
  Substring and numeric patterns

	▼	
	▼	
	▼	

Enter the search criteria.

An Event will be generated only if the event description matches the given condition.

For example: 'Manager = 192.168.1.4'

9. Select/enter the appropriate event property details in the **Event Properties** field, and then click **Add**.
10. In the **Correlator Event/Action Details** pane, move the pointer over the newly created event name. Netsurion Open XDR displays the correlator event details in a pop-up window.

**CORRELATOR RULE DETAILS**

Name:   Active

Description:

---

**CORRELATOR EVENT/ACTION DETAILS**

FileTransferF	
Log Type	System
Event Type	Information
Category Id	
Source	System
Event Id	3279
User	Karen
Computer	MCLOON-II
Domain	
Description	

If  Event

within 30 second

Event

tion

ction

Place the Pointer

11. In the **Correlator Event/Action Details** pane, click the **Add Action** hyperlink. (If Netsurion Open XDR real-time Correlator is installed). The Action Properties window will be displayed as shown below:

Internet Explorer - Properties

### ACTION PROPERTIES

Type of action  Generate event  Run script

Label\*

Log Type  ▼

Event Type  ▼

Category

Source  ..Previous Reference.. ▼

Event Id\*

User  ..Previous Reference.. ▼

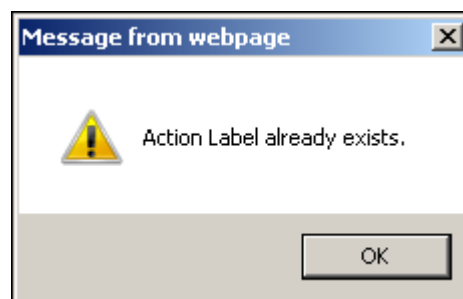
Computer  ..Previous Reference.. ▼

Domain  ..Previous Reference.. ▼

Description   
(select to insert a previous reference in description) ..Previous Reference.. ▼

ADD CANCEL

12. Enter an appropriate label name in the **Label** field for the event action. This is a mandatory field.



**Note**

The Label name in event properties and action properties cannot be the same. If you enter the same name, Netsurion Open XDR displays an error message.

13. Enter/select the appropriate details in the **Action properties** pane.
14. Click the **Previous Reference** dropdown to select the same values that you have entered in the **Event Properties** field.
15. In the **Description** field, describe the actions on the generated event.

### ACTION PROPERTIES

Type of action  Generate event  Run script

Label\*

Log Type  ▼

Event Type  ▼

Category

Source   ▼

Event Id\*

User   ▼

Computer   ▼

Domain   ▼

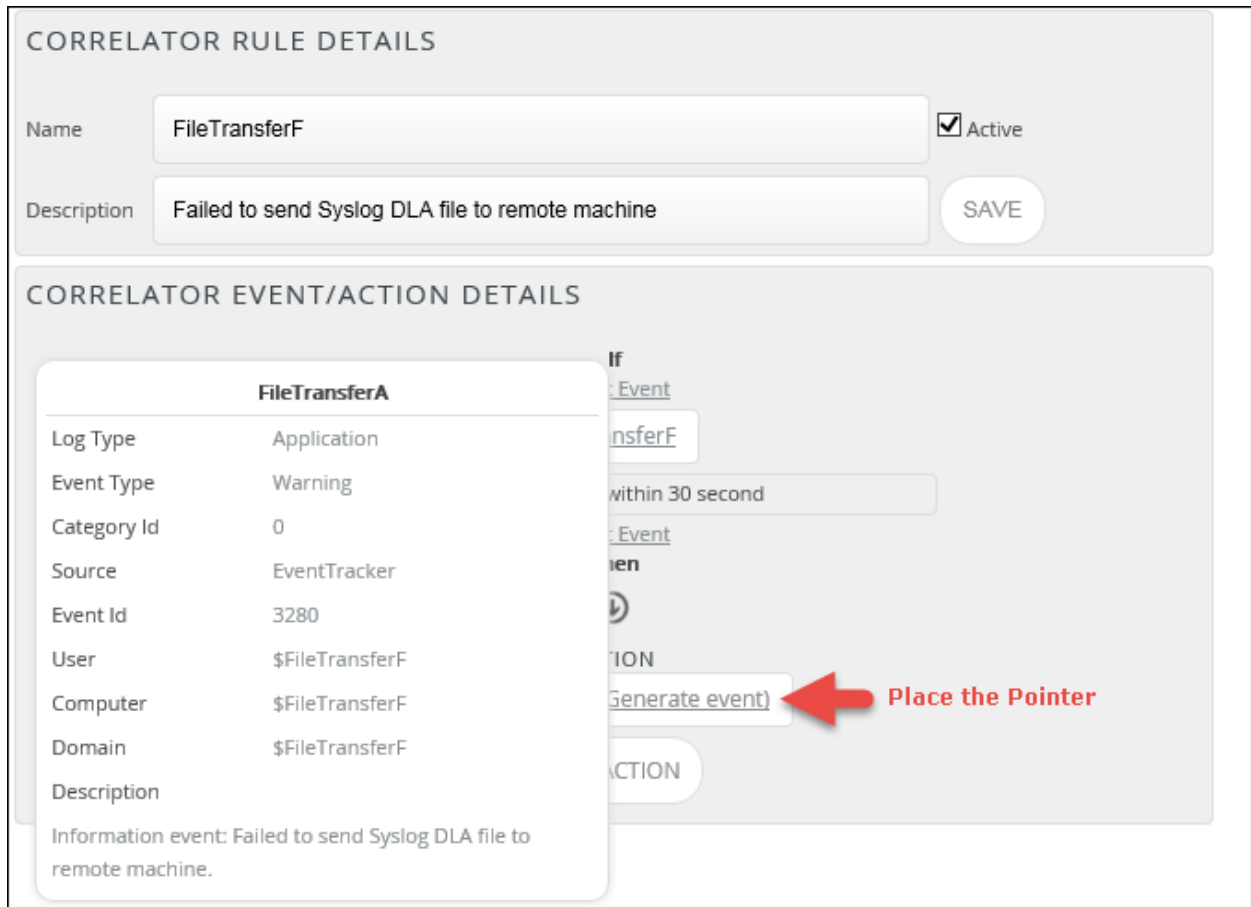
Description

(select to insert a previous reference in description)  ▼

**Note**

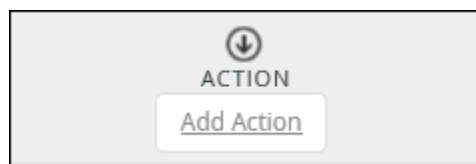
In this field, you can add the substring from the Event Properties description to look for more specific results to apply the correlation rule.

- Click the **Add** button.
- In the **Correlator Event/Action Details** pane, move the pointer over the newly created action name. Netsurion Open XDR displays the correlator action details in a pop-up window.



## 4.2 Action Item to Run a Script

- Select or create a new correlator rule. For example: UNIXRootLogin.
- Click **Add Action**.



- Select the **Run Script** option. The Action Properties window will be displayed as shown below:

The screenshot shows the 'ACTION PROPERTIES' dialog box in Internet Explorer. The 'Type of action' section has two radio buttons: 'Generate event' and 'Run script'. The 'Run script' option is selected and highlighted with a red box. Below this, there are fields for 'Label\*', 'Script type\*' (set to 'VB'), and 'File location\*' with a 'BROWSE' button. The 'Parameters\*' section is empty, with up and down arrows and a trash icon. Below this is the 'PARAMETERS' section with two radio buttons: 'Column' (selected) and 'Static'. There are input fields for each, and an 'ADD PARAMETER' button. At the bottom right, there are 'ADD' and 'CANCEL' buttons.

4. Select/Enter the mandatory criteria in the **Action Properties** window.
5. In the **Parameters** pane, select the **Column** or **Static** option.
6. If the **Column** dropdown is selected, enter the relevant options and then click **Add Parameter**.
7. Click **Add**.

The screenshot shows the 'ACTION PROPERTIES' dialog box in Internet Explorer. The 'Type of action' section has two radio buttons: 'Generate event' and 'Run script'. The 'Run script' option is selected and highlighted with a red rectangular box. Below this, there are several input fields and buttons: 'Label\*' (empty text box), 'Script type\*' (dropdown menu showing 'VB'), 'File location\*' (empty text box with a 'BROWSE' button to its right), 'Parameters\*' (empty list area with up/down arrows and a trash icon), and a 'PARAMETERS' section with two radio buttons: 'Column' (selected) and 'Static'. There are also 'ADD PARAMETER', 'ADD', and 'CANCEL' buttons at the bottom right.

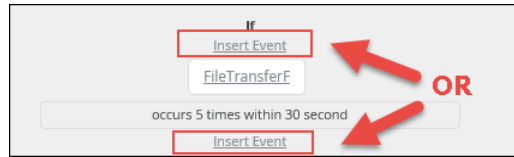
8. The existing script is generated with relevant parameters.

### 4.3 To Edit a Correlation Rule

1. Select an existing rule.
2. Enter the required changes in **Correlation Rule Details**.
3. In the **Correlator Event/Action Details** pane, click the existing event, update the required information, and then click **Save**.

#### Note

You can also insert an event after or before an existing event property. Hover over the event to insert another event.



4. Click the existing **Generate Event in Action**, update the required information, and then click **Save**.

**CORRELATOR RULE DETAILS**

Name:   Active

Description:

---

**CORRELATOR EVENT/ACTION DETAILS**

**IF**

[Insert Event](#)

[Insert Event](#)

**Then**

⬇

**ACTION**

5. To add another action, click the **Add Action** hyperlink.

**CORRELATOR RULES**

AVAILABLE RULES

- \$ExcessiveC672R
- \$ExcessiveD4656R
- \$ExcessiveD560R
- \$ExcessiveF4656R
- \$ExcessiveF560R
- \$ExcessiveU4656R
- \$ExcessiveU560R
- EntLogonfail1\_Rule
- excessive4771R
- excessive675R
- FileTransferF
- InitRule1
- InitRule2
- IntrusionRule1
- pingRule1
- UNIXRootLogin

**CORRELATOR RULE DETAILS**

Name:   Active

Description:

---

**CORRELATOR EVENT/ACTION DETAILS**

**IF**

[Insert Event](#)

[Insert Event](#)

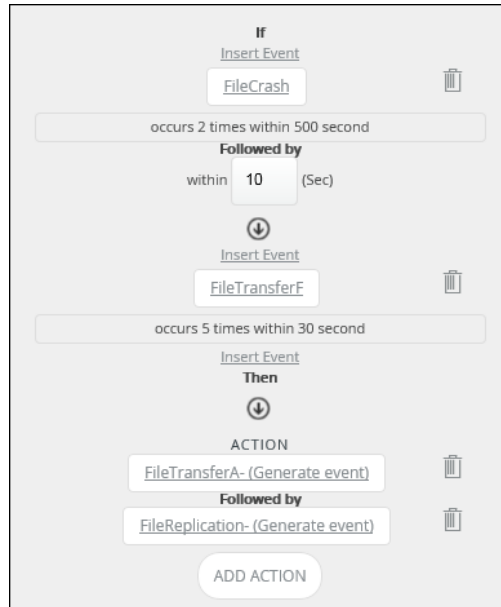
**Then**

⬇

**ACTION**

6. Enter the required information and then click **Add**. You can add multiple numbers of events and actions.



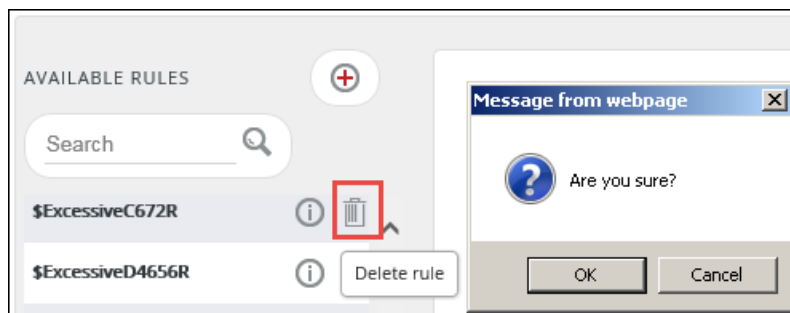


**Note**

If you want to delete an Action or an Event, click the Delete icon.

## 4.4 To Delete a Correlation Rule

1. To delete any rule, click the **Delete** icon adjacent to the rule.




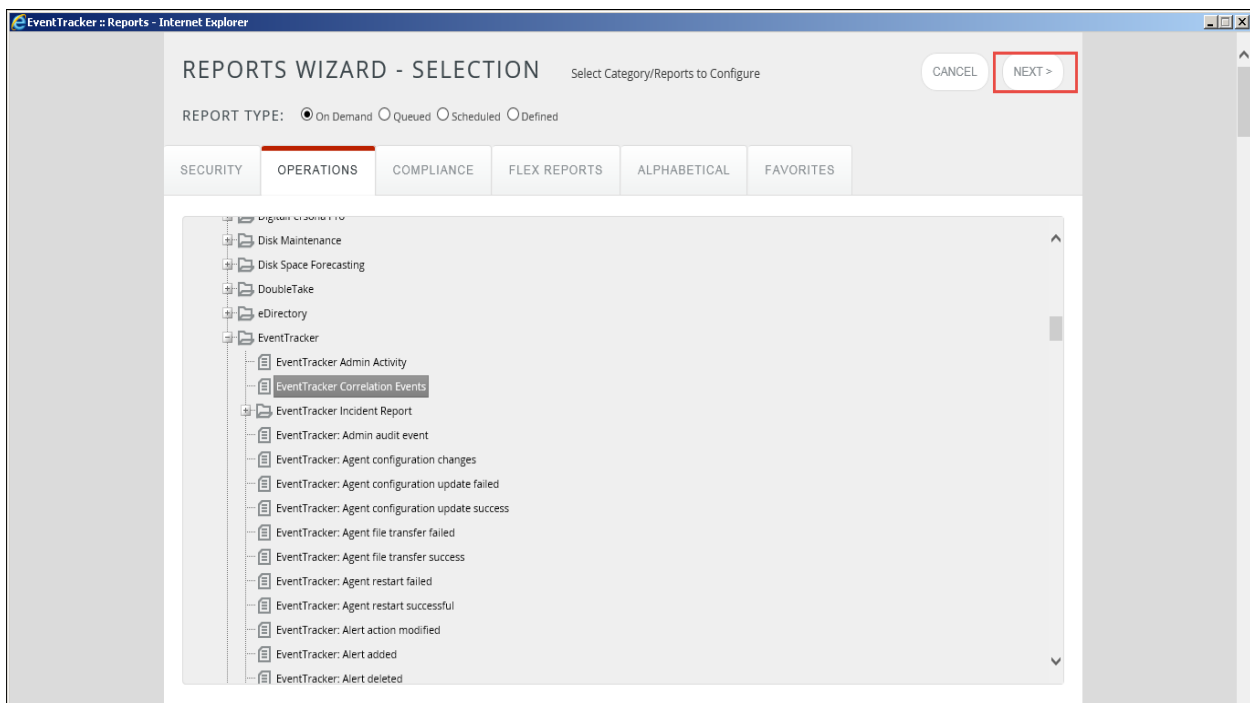
2. Click the **OK** button.

## 5 Generate Netsurion Open XDR Correlation Events Report

For correlator rules to be visible under **Reports > Operations**, select any existing rule and save it. This is applicable for on-demand correlators only.

### 5.1 Configure Reports

1. Log in to **Netsurion Open XDR Enterprise**. Select **Reports**, and then select **Dashboard or Configuration**.
2. Select the **New** icon , and then select the **Operations** tab.
3. In the '**Reports**' tree, select **Netsurion Open XDR** node and expand it.
4. Select **Netsurion Open XDR Correlation Events**, select **Report Type**, and then click the **Next** button.

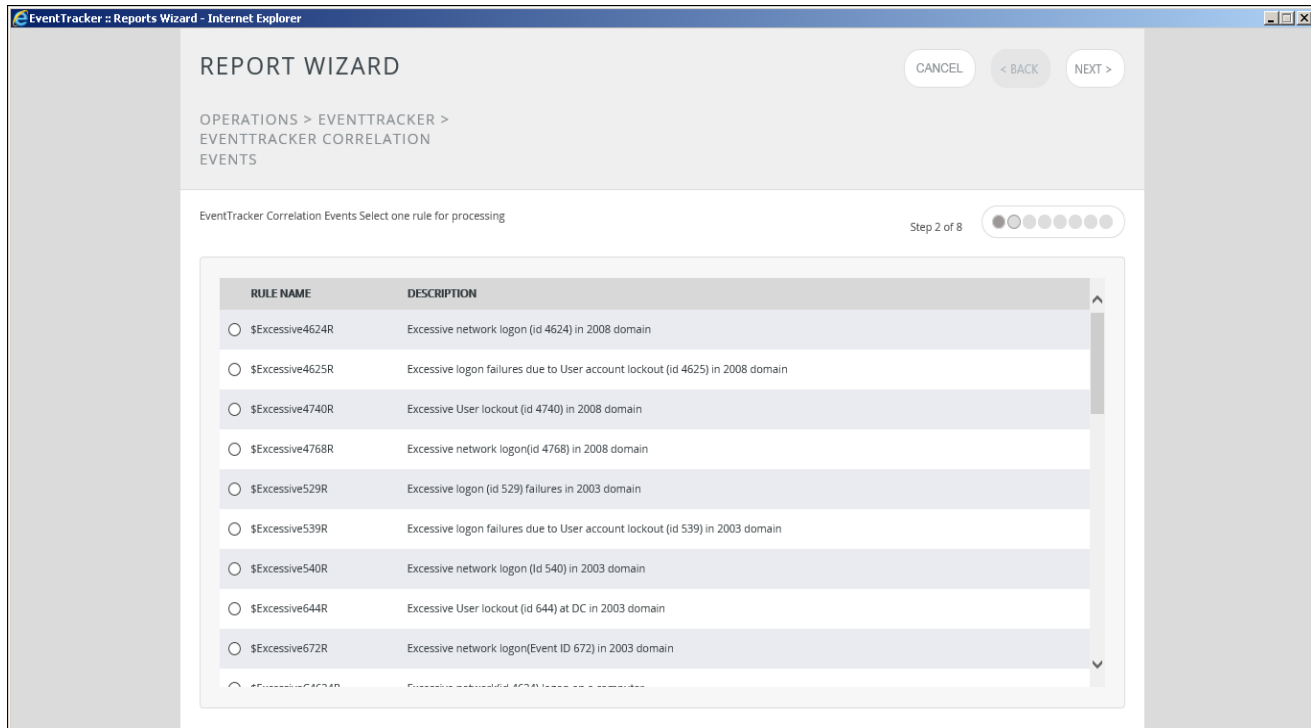


#### Note

You will find Netsurion Open XDR Correlation Events Report only if you install the on-demand Correlator.

(OR)

1. Right-click **Netsurion Open XDR Correlation Events**.
2. Select the **On Demand/ Queued / Scheduled /Defined** option.
3. Netsurion Open XDR displays the **Reports Wizard**.
4. Click the **Next >>** button.
5. Select any rule for processing, and then click the **Next** button.



You can now proceed further and configure the required correlation rule and the relevant reports will be generated.

## 6 Examples

### 6.1 Correlation of Two Events

This example will help the user search for a matched string extracted from two different events used for correlation. In the Rule Section Pattern field, a string comparison is required. A sample configuration is shown below.

```
[EVENT]
Label = Event4625
LifeTime = 300
LogType = 2
EventType = 5
CatId =
Source =
ComputerName =
EventId = 4625
User =
Domain =
Description = &<Data Name='TargetUserName'>&&</Data>&
[End]

[EVENT]
Label = Event4624
LifeTime = 300
LogType = 2
EventType = 4
CatId =
Source =
ComputerName =
EventId = 4624
User =
Domain =
Description = &<Data Name='TargetUserName'>&&</Data>&
[End]

[ACTION]
Label =ActionEvent555
DO = GenerateEvent
LogType = 1
EventType = 2
CatId = 0
Source = EventTracker
ComputerName =
EventId = 555
```

```

User =
Domain =
Description = This event indicates a successful login after 3 logon
failure by an user$Event4625.Description&<Data
Name='TargetUserName'>&&</Data>& .
[End]
[RULE]
Label = sucessfulllogin
Description = sucessfulllogin after failure
Pattern =
Event4625:3,Event4624:1,$Event4625.Description==$Event4624.Description
Action =ActionEvent555
[End]

```

#### Note

- At present, the rule condition is supported for EQUAL (==) and NOTEQUAL (!=).
- UI is not available to configure this in the rule section of INI.

## 6.2 Search for a Particular Substring

This example will help the user to search for a specific description in the event properties of resultant events. For this, you need to enter the required description as a substring in the **Look for substring** option of **Event Properties- Description**.

```

[EVENT]
Label: Excessive4625
Life Time (Seconds):300
Occurrences: 10
Log Type:
Event Type:
Category:
Source: System
Event ID: 4625
User:
Computer: MCLOON
Domain: TOONS
Description: Account Locked Out
[End]

[ACTIONS]
Label: Excessive4625A
Log Type: Security
Event Type: Audit Failure
Category:

```

```

Source: Intrusion
Event ID: 3258
User: System
Computer: $Excessive4625F
Domain: $Excessive4625F
Description: Intrusion Detection: Excessive logon failures due to User
account lockout in your enterprise: \N\N For more information about this
condition\N Generate a report on event ID 4625 using EventTracker - Log
Search
[End]

```

The above rule set says that the events received from Netsurion Open XDR are to be monitored that possess the Event ID **4625**, and contain a description as **Account Locked Out**. If that event occurred 10 (pattern) times in 300 (lifetime) seconds, then the action **Excessive4625A** will be fired which will generate a new event **3258**.

The new event will be generated with the specified properties (Log type=security, Event Type=Audit Failure, and so on). The Parameter fields (\$) in the action properties will be replaced by appropriate values from the actual event.

## 6.3 Add Event Properties Description in the Action Event

### 6.3.1 In the Presence of Event Source Description

In some cases, you may need to reproduce some values from the source event in the event generated by the correlator. The following example will show you how to use the parameter to write an **Action event** description using details from Event Properties.

```

[EVENT]
Label: IntEvt1
Life Time (Seconds):300
Occurrences: 5
Log Type: Security
Event Type: Audit Failure
Event ID: 676
Description: Look for substring sequence -Client Address Followed by 15
[End]

[ACTIONS]
Label: Intract1
Log Type: Security
Event Type: Audit Failure
Category: 0
Source: Intrusion
Event ID: 3251
User: SYSTEM

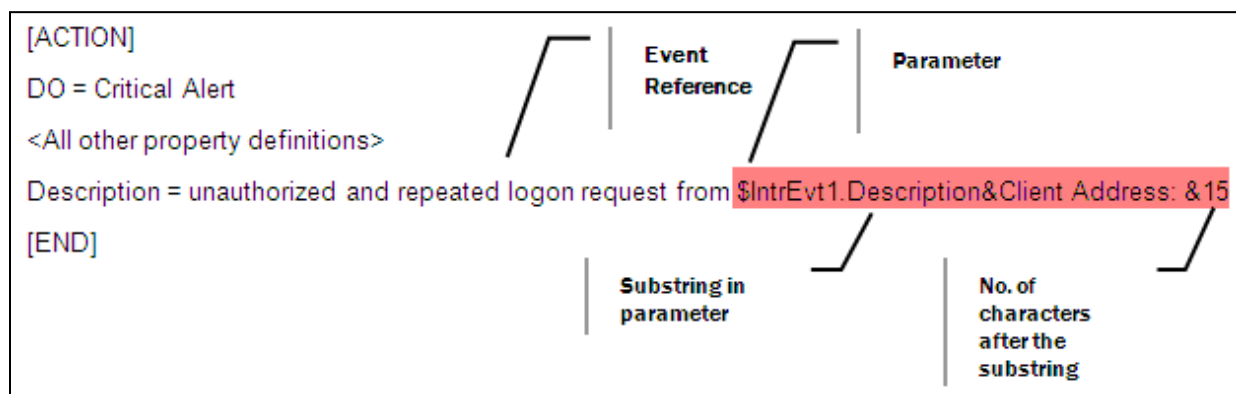
```

```
Computer: $IntrEvt1
Domain: $IntrEvt1
Description: Critical alert- Intrusion detected.\N\N\N An unauthorized
and repeated logon request from $IntrEvt1.Description&Client Address:
&15.\N\N It may be due to sophisticated hacking attempt. Please
investigate and if required block the IP address on the firewall
[End]
```

The above rule set says that the events received from Netsurion Open XDR to be monitored that possess the Event ID **676** and contain **Client Address** up to **15** characters in the description. If that event has occurred 5 (pattern) times in 300 (lifetime) seconds, then the action **Intract1** will be fired which will generate a new event **3251**.

The new event will be generated with the specified properties (Log type=Security, Event Type=Audit Failure, and so on). The Parameter fields (\$) in the action properties will be replaced by appropriate values from the actual event.

In simple terms, while defining rule sets, you can make use of the existing event details by its name as the reference. The parameter references can use string substitutions also.



### 6.3.2 In the Absence of Event Source Description

If the 'Event properties' description in **Look for substring** is left blank, then the generated action event will display the source event description. Here, the action event will extract the description from an event that has occurred at the last in the given lifetime. The following example will show you the use of parameters to write an 'Action Properties' description.

```
[EVENT]
Label: IntEvt1
Life Time (Seconds):300
Occurrences: 5
Log Type: Security
Event Type: Audit Failure
Event ID: 676
```

```

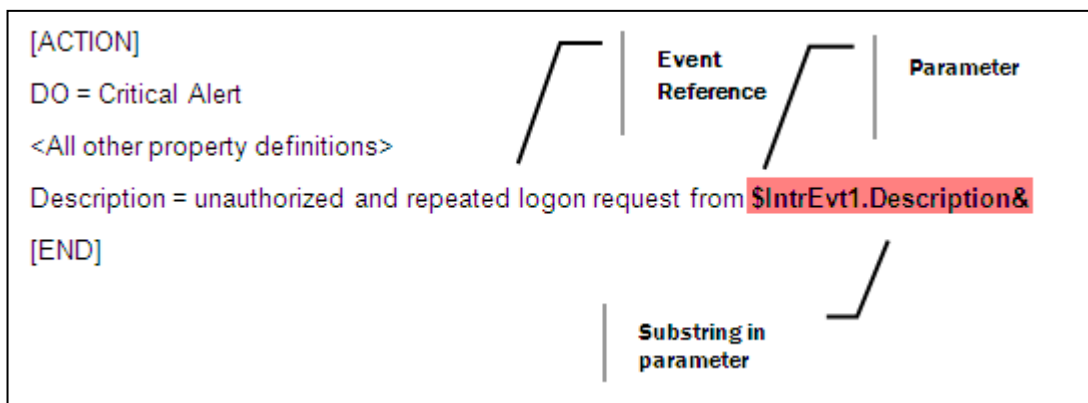
Description:
[End]

[ACTIONS]
Label: Intract1
Log Type: Security
Event Type: Audit Failure
Category: 0
Source: Intrusion
Event ID: 3251
User: SYSTEM
Computer: $IntrEvt1
Domain: $IntrEvt1
Description: Critical alert- Intrusion detected.\N\N\N An unauthorized
and repeated logon request from $IntrEvt1.Description&.\N\N It may be due
to sophisticated hacking attempt. Please investigate and if required block
the IP address on the firewall
[End]

```

The above rule set says that the events received from Netsurion Open XDR to be monitored that possess the Event ID **676**. If that event occurred 5 (pattern) times in 300 (lifetime) seconds, then the action “**Intract1**” will be fired which will generate a new event **3251**.

As the source event description is left blank, the description ‘**\$IntrEvt1.Description**’ in action properties will fetch the description from the event that has occurred at the last in the given duration. In this example, the description of the 5<sup>th</sup> event will be displayed in the action event.





## 7 Steps to Enable Group-Level Event Correlation

To enable the correlation for group level:

1. Update the key "CorrelGroupBase" in tbl\_Config to True or 1 (SQL Database).
2. Navigate to the ...install directory\EventTracker\ETCorrel path.
3. Next, in **ETCorrel.ini**, use the "@@" character for group consideration in the "ComputerName =@@" column of [EVENT] section.

```
#####
# Prism Microsystems, Inc
# eMail : support@prismmicrosys.com
#####

[CORREL]

CacheSize = 50000

EventLifeSecs = 60

Debug = 0

ActionEventDestn = 127.0.0.1

[End]

#-----
#Rule : Excessive logon failures due to bad password in 2003 domain
#-----

[EVENT]

Label = excessive675

LifeTime = 300

LogType = 2

EventType = 5

CatId =
```

```
Source =  
  
ComputerName = @@  
  
EventId = 675  
  
User =  
  
Domain =  
  
Severity =  
  
Description =  
  
Comments =  
  
[End]  
  
[ACTION]  
  
Label = excessive675A  
  
DO = GenerateEvent  
  
Destination = 127.0.0.1:14505  
  
LogType = 2  
  
EventType = 5  
  
CatId = 0  
  
Source = Intrusion  
  
ComputerName = $excessive675  
  
EventId = 3253  
  
User = $excessive675  
  
Domain = $excessive675  
  
Severity = 1  
  
Description = Intrusion is detected - Excessive logon failures due to  
bad password \N\N Number of log failures in your enterprise have crossed  
the limit. \N\NPlease generate a report on event id 675 to verify that  
which system and user is trying responsible for intrusion.  
  
Comments =
```

```
[End]

[RULE]

Label = excessive675R

Description = Excessive logon failures due to bad password in 2003
domain

Pattern = excessive675:10

Action = excessive675A

[End]
```

4. After making the changes, restart the **Event Correlator** service.

After applying the update, for the event rule where the computer name is given as @@, it will consider the events based on group level.

## About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection 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 & Response (MXDR). Learn more at [www.netsurion.com](http://www.netsurion.com).

## Contact Us

### Corporate Headquarters

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

### Contact Numbers

Use the [form](#) to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	<a href="mailto:SOC@Netsurion.com">SOC@Netsurion.com</a>
Managed XDR Enterprise MSPs	<a href="mailto:SOC-MSP@Netsurion.com">SOC-MSP@Netsurion.com</a>
Managed XDR Essentials	<a href="mailto:Essentials@Netsurion.com">Essentials@Netsurion.com</a>
Software-Only Customers	<a href="mailto:Software-Support@Netsurion.com">Software-Support@Netsurion.com</a>

<https://www.netsurion.com/support>