# Trap

## Create and Configure Traps

In the system devices or locations will generate alarm based on the predefined trigger. The application generates all alarms, notifications and actions based on Attributes. So, the first step to creating support for a new trap is to ensure there is an attribute created in the application. This step is completed on the Attribute Manager page which is in the Settings group menu.

* + Name – Define the name of the trap attribute. This is typically a unique name which is easy to find and manage when reported in the Alarms and Calendar features of the application.
  + Define the Category where this attribute will be visible when reviewing the full attributes list.
  + Choose the Value Type of the trap to be delivered from the device. In most cases, this type will be set to String.
  + Usage – Choose the Device checkbox. Only device traps are supported in the application. This attribute will be used in other sections below to fully configure the trap object in the application.

## Create Trap Data Elements

Once the trap attribute is defined in the application, the user can go to the Monitoring – Monitoring Templates page to create support for the actual trap object from the device. Examples of predefined traps can be found in the monitoring templates that start with the string “Trap”. Create a new monitoring template which will contain the list of traps to be created for your device. There are two ways to define the individual trap attributes in the monitoring template as documented below.

## Traps Defined Manually

Users can manually define a trap attribute in the monitoring template by following these steps. Please refer to working examples of traps in the preconfigured Monitoring Templates if more information is needed on how to manually create a trap attribute:

* + Choose the Attribute from the application Attribute Manager which will be used for tracking the trap object sent from the device.
  + Define an alias for this attribute. This is not required but may be a way to provide a user- friendly name to a more complex attribute name. The Alias name will be used for reporting in alarms and calendar events.
  + Data Type should be set to Scalar.
  + Monitor Type should be set to SNMP Trap.
  + Parameters – Trap OID should be the OID from the device MIB which represents the trap alarm sent by the device. Specific is a configuration setting which is defined in the manufacturer MIB

## Traps Imported from MIB

An alternative to the manual creation of the trap object in the application is to use the Import from MIB option when creating attributes. This method is much easier to use and is recommended for trap configuration activity. To use this method of creating support for traps, follow these steps below:

* + Create a new Monitoring Template or open an existing template which will contain the trap definitions.
  + On the Attributes Tab, click the Add button.
  + At the top of the Add Attribute page turn on the Add Attribute from MIB checkbox.
  + Browse to the file which is the MIB file which contains the trap definitions to support.
  + Select the checkbox next to the trap objects which will be imported.
  + Assign the application Attribute which will be used to map to the Trap object. A list of available Attributes is in the dropdown list in the Attribute column of the table.
  + Click the Submit button.

The selected traps will be created in the monitoring template and can be assigned to devices.

## Define Trigger for Trap

The nature of an SNMP Trap is to report a condition with the device and report the alarm condition to the monitoring application. The steps in the sections above will configure the application to receive the trap from the source device, but for the trap to be reported to users you need to define the Trigger for the trap event.

Defining a Trigger for a trap attribute is the same as defining a Trigger for a standard polled data element from a device. On the Monitoring Template where the Traps are defined, select the Triggers tab and click the New button to define a new Trigger. Key elements of the SNMP Trap Trigger are as follows:

* + Name – Name of the Trigger. This trigger name will appear in the Alarms and Calendar when the trap event is detected.
  + Severity – Alarm severity to assign to the event when the trap is received for the device.
  + Rules – Select the Trap attribute or combination of trap attributes which will cause this Trigger to be enabled.

Click Submit to save the Trigger definition. When this trigger event is enabled the device will be set to the defined alarm severity in the trigger rule.

## Define Recovery Rules for Trap

When traps are received by the application and a trigger is enabled to set an alarm for a device, there needs to be an automated way for the trap alarms to be cleared from the alarm panel when the device reports the original trap condition no longer exists. Users can configure these recovery rules within the Triggers page for the trap alarm.

On the New Trigger definition page, there is a Recovery Rules section which is used to define the Trap events which will clear the alarm condition. Essentially, when the recovery rules events are received for the device, the original trap event will be cleared for the device. This clearing of the trap event will reset the trap to Normal condition for the device which eliminates an entry in the alarm panel for the device.

**Note**: When defining the recovery rules, there are options to use compound logic the AND|OR buttons to require multiple trap events to clear the original trap alarm.

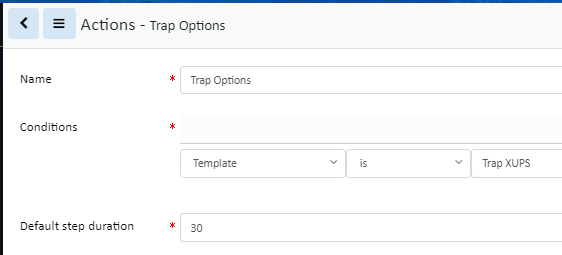
## Define Custom Messages for Trap

On the New Trigger definition page there is an option to deliver a text string along with the trap alarm. Using the Message Format field on the new trigger page, users define the text string which will be sent with the trap alarm when it is generated. This text string will appear in the Alarm panel and the Calendar entry for the alarm generated for the device.

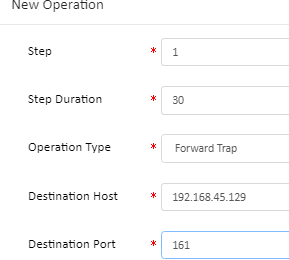
## Configure Trap Forwarding

Users may want for the application to collect SNMP Traps from devices and then forward these traps to a third-party application for further processing. For these use cases, the Actions feature is used to define Trap Forward rules.

Create a New Action by selecting the Template, Trigger or Alarm which contains the SNNP Trap you want to forward to a third-party application.



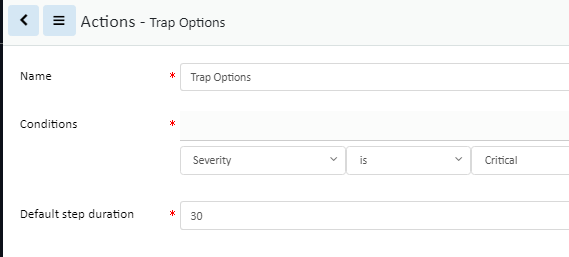
Define an Operation Rule where Operation Type is set to Forward Trap and the Destination Host|Ports are for the server which should receive the trap.



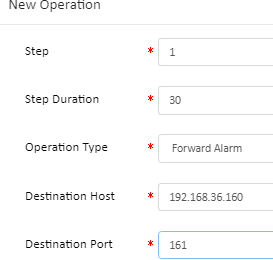
## Generate Trap to 3rd Party Application

The Visual Data Center application is capable of delivering SNMP Traps for any alarm detected within the application. Alarms are generated using the Trigger feature so they may be simple threshold alarms, complex triggers involving multiple conditions or traps received from devices managed within the application. In any of these cases, the Visual Data Center application can notify a third-party application with an alarm which is in the format of an SNMP Trap.

In the example below, an Action is created for any alarm generated in Visual Data Center which has a severity of Critical.



To forward this alarm condition to a third-party system users will create a new Operation with this Action where Operation Type is set to Forward Alarm and the Destination Host|Port are set for the server which should receive the Alarm trap generated by Visual Data Center.



## Trap Troubleshooting

For traps to be delivered by an end device, received by Visual Data Center and processed correctly requires proper configurations for traps across devices. Please reference these important notes for configuring traps to work properly with the application.

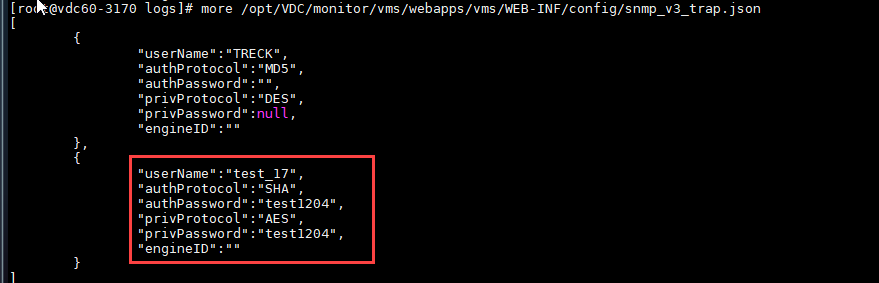
## Device Configurations

* + Ensure the end device is configured to deliver traps to the Visual Data Center Probe server. Many devices refer to this as the Trap Receiver configuration and setup. By default, the Visual Data Center trap listener is configured to listen on port 162.
  + For SNMP version 1 traps, ensure the Community strings are defined for the end device.
  + For SNMP version 3 traps, more configuration elements are required:
    - The definition of the Trap Receiver (Visual Data Center Probe) will require a user name to be included in the setup.
    - The version 3 user name has different Security options for authentication and privacy. A single setting must be used for all devices using SNMP version 3 communication to Visual Data Center:
      * No Auth, No Priv
      * Auth, No Priv
      * Auth, Priv

## Probe Server Configuration – SNMP Version 3 Only

If SNMP Version 3 traps are being sent from devices, the Visual Data Center probe server must have the following configuration file updated to align with the settings defined on the end device. All devices at the customer site must communicate with the same SNMP version 3 communication settings. The following file is used to define the communication settings for version 3 traps:

/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/snmp\_v3\_trap.json



"userName":"",

"authProtocol":"",

"authPassword":"",

"privProtocol":"", "privPassword":null, "engineID":""

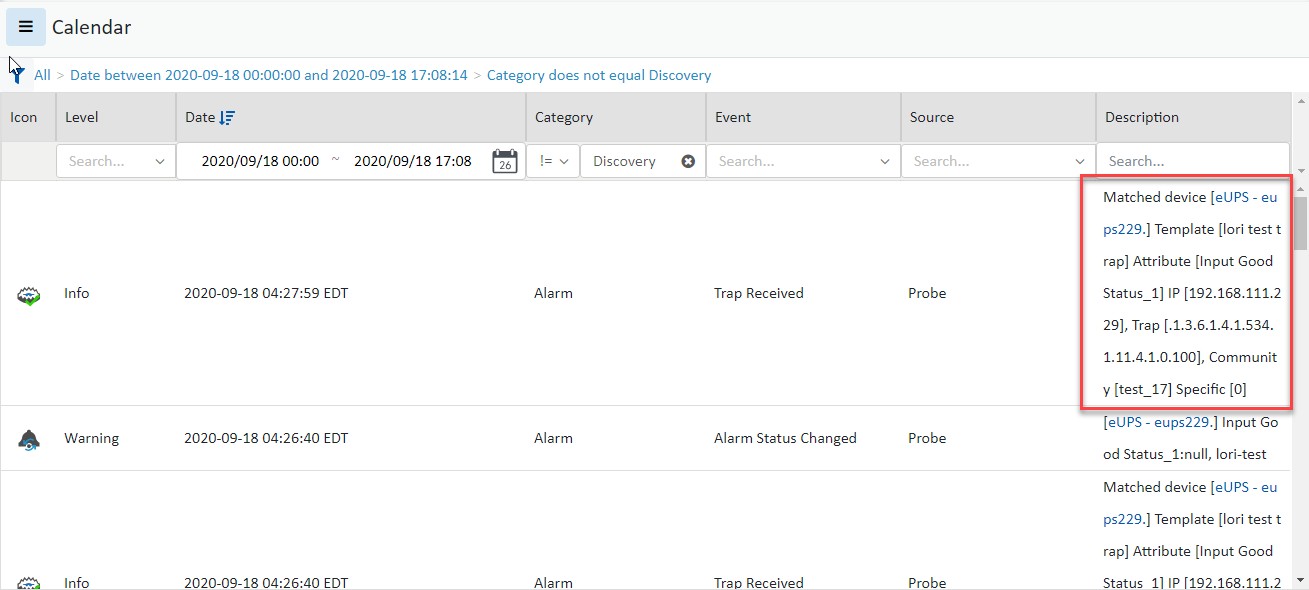
All values entered to this configuration file should be entered between the “” after the colon.

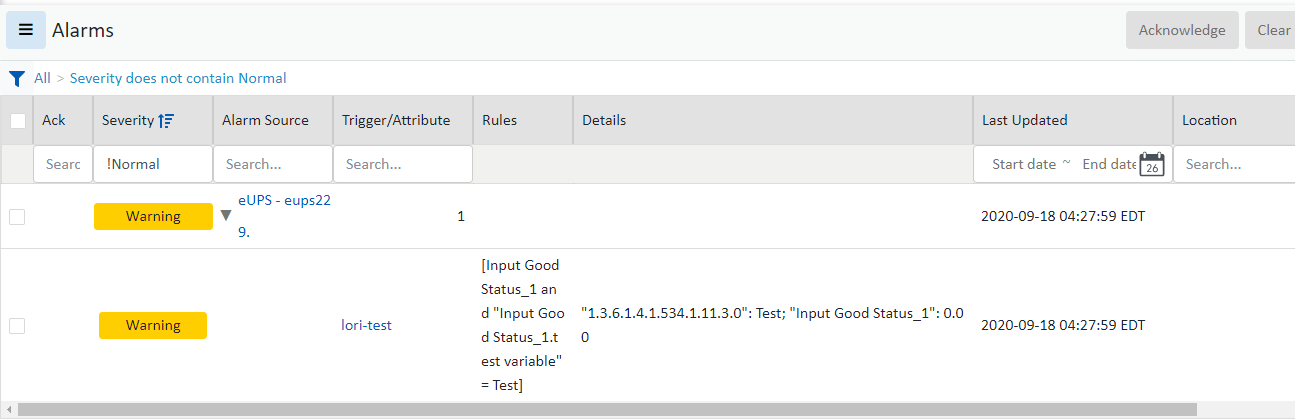
* + userName – Insert the SNMP version 3 user configured on the end device which is delivering the trap.
  + authProtocol – Enter either MD5 or SHA.
  + authPassword – If a password is required for the authentication then enter here.
  + privProtocol – Enter either AES or DES here.
  + privPassword – If a password is required for the privilege setting then enter here.
  + engineID - Engine ID of the authoritive snmp entity (trap sender). If trap sender's engineID can be ignored, null value can be used

If this configuration file is updated, the vms process (on the probe server) MUST be restarted.

1. Login to the server as root
2. ps -ef | grep vms
3. kill -9 the process ID assigned to the vms process in the output of the first command
4. su - vdc -c "cd /opt/VDC/monitor/vms/bin;./vms start >/dev/null 2>&1"

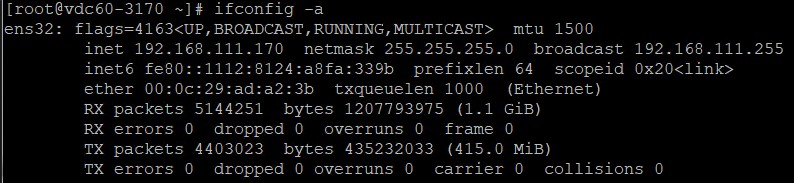
If there is not an existing monitoring template it needs to be created. Once a monitoring template exists, users must enable the template and monitoring for the device and then the v3 traps can be received.



Triggers created by the traps are generated when traps received.

### Get Number of Traps Coming into Server

To get the number of traps coming into the server from a specific IP and port run the following command as root:

tcpdump -i ens32 -w /tmp/troubleshoot.pcap -vv -A -T snmp -s 0 "(src 192.168.111.229 and dst port 162)" Where ens32 is the name of the NIC port in use on the application server.

### Trap Log Information

The trap log in the probe server will contain details related to all traps received from end devices. The following commands are helpful in working with the trap log to troubleshoot trap processing:

* + tail -f /opt/VDC/monitor/vms/logs/trap.log – Opens a session where new traps written to the log will be displayed on the screen.
  + grep -i [DEVICEIP] -A 20 -B 20 /opt/VDC/monitor/vms/logs/trap.log – Replace the [DEVICEIP] with the device IP address sending the traps to the probe server. THIs will limit the information to review from the log to a targeted device. **Note**: The -A 20 and -B 20 options will show 20 lines above and 20 lines below the line which matches the device IP Address.

The probe server will attempt to match all traps received with traps configured in Visual Data Center.

* + If the device IP in the trap matches a device IP in the application.
  + If the trap OID matches an ACTIVE trap attribute set for the device. Please note this requires the monitoring template is activated for the device AND the actual trap within the monitoring template is enabled.

If the analysis results in a mismatch, the trap log will indicate the trap does not match any devices in the application and the trap will be discarded from further processing.

If the analysis results in a match, the trap will be processed based on configuration of the trap attribute.

* + An entry will be written to the Calendar module with the Event equal to Trap Received.
  + If configured, an alarm level will be assigned to the device.
  + If the trap is configured with Recovery Rules then those will be processed as well to cancel previously set traps for the device.

for each trap object being sent to the application as an alarm. Item Value is used in some cases to match the value assigned in the trap to a configuration with the attribute defined in the application.

* + Variable Bindings – In some cases traps will be dependent on other objects in the SNMP MIB. If the trap object being defined has a variable binding then click the Add button and define the Name, OID and Value type fields.
  + Status – Determines if the application will process this trap definition for the assigned devices.