CONNECTWISE

SNMP Trap Receivers Tab in the Control Center

Overview

The SNMP Trap Receivers tab of the SNMP Traps screen is located in the Network Probe tile. The SNMP Trap Receivers tab enables you to create new SNMP trap filters to collect information. The SNMP Traps Received tab is located next to the SNMP Trap Receivers tab that displays all the SNMP traps that have been received based on the trap filters you have created on the SNMP Trap Receivers tab.

SNMP Trap Receivers Tab Breakdown

The following explains each area of the SNMP Trap Receivers tab as well as how to navigate to it:

1. From the **Control Center**, select **Browse** > **Clients** tab > **Computers** tab.
2. Double-click on the network probe computer. You can determine the probe machine by locating the device with a **Network Probe**

icon appearing in the **Flags** column. The **Computer Management** screen is displayed.

3. Select the **Automation**

workspace and then click on the **Network Probe** tile.

4. Click on **SNMP Traps** from the navigation pane and then select the **SNMP Trap Receivers** tab.

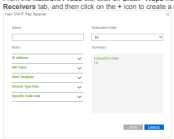
Trap Receivers	
Name	Displays the name of the SNMP trap receiver filter.
Evaluation Order	Displays the number representing the order in which the SNMP trap receiver filter will be evaluated.
Add	Enables you to create a new SNMP trap receiver filter.
Edit	Enables you to modify an existing SNMP trap receiver filter.

Delete	Enables you to remove an existing SNMP trap receiver filter.
Details	
Name	Displays the name of the SNMP trap receiver filter.
IP Address (Regular Expression)	Displays the IP address that the SNMP trap receiver filter will search.
OID	
Comparison	
Result	
Generic Comparison	
Generic Result	
Specific Comparison	
Specific Result	

Add SNMP Traps

To add an SNMP Trap:

1. From the **Network Probe** tile, click on **SNMP Traps** from the navigation pane, select the **SNMP Trap Receivers** tab, and then click on the **+** icon to create a new trap receiver.



2. Enter the desired **Name** for the trap you want to create.
   Note: The **IP Address**, **OID Value**, **Generic Type Rule** and **Specific Code Rule** can all be used in conjunction with each other or individually.
3. If applicable, enter a comma-separated list of IP addresses of the printer(s) or router(s) generating the trap(s) in the **IP Address** field. If a value is not entered into this field, it will ignore the IP address. If you only have a few IP addresses, the easiest method is to enter them in a comma-separated list, such as 10.30.56.90, 10.30.56.95, 10.30.56.122. A range of numbers is also acceptable.
   Here are some examples:
   - Example A: You want addresses between 123.45.6.70 and 123.45.6.90, inclusive. Enter in the following format, 123.45.6.[70-90].

   - Example B: You want to add a filter that allows every IP address on a /24 subnet. Enter in the following format, 123.45.6.*
   - Example C: An alternative way of entering a comma-separated list (10.30.56.90, 10.30.56,95 and 10.30.56.122) is to enter the list in the following format: 10.30.56.[90, 95, 122].
4. If applicable, click on **OID Value** and enter the OID value or click on the **Ellipsis** button to select from the OID selector and then:
   i. Select the appropriate check condition from the **Check Condition** drop-down field.
   ii. Enter the result that you want the trap to report on into the **Result** field.
5. For an alert to be generated when a trap is received, select the desired alert template from the **Select Alert template** drop-down. If there is not an appropriate template available, you can choose to create a new template. For additional information on how to create a new template or edit the alerts on an existing template, refer to Configuring Alert Templates.
   i. Optional: Enter an **Alert Message**.
6. If applicable, expand the **Generic Type Rule** and then:
   i. Select the **Check Condition** from the drop-down menu.
   ii. Enter the **Result** that you want the trap to report on. See the table below for more information on generic type filters:

Trap Name/Number	Description
coldStart (0)	Indicates that the device has rebooted. All management variables will be reset; specifically, Counters and Gauges will be reset to zero (0).
warmStart(1)	Indicates that the agent has reinitialized itself. None of the management variables will be reset.
linkDown(2)	Sent when an interface on a device goes down. The first variable binding identifies which interface went down.
linkUp(3)	Sent when an interface on a device comes back up. The first variable binding identifies which interface came back up.
authenticationFailure(4)	Indicates that someone has tried to query your agent with an incorrect community string; useful in determining if someone is trying to gain unauthorized access to one of your devices.
egpNeighborLoss(5)	Indicates that an Exterior Gateway Protocol (EGP) neighbor has gone down.
enterpriseSpecific(6)	Indicates that the trap is enterprise-specific. SNMP vendors and users define their own traps under the private-enterprise branch of the SMI object tree.

7. If applicable, expand the **Specific Code Rule**. Typically, specific codes are manufacturer specific.
   i. Select the **Check Condition** from the drop-down menu.
   ii. Enter the **Result** that you want the trap to report on.
8. If applicable, you may change the **Evaluation Order** from the default value of 10 according to your needs. The evaluation order determines the priority on which the traps are evaluated. An evaluation order of 1 will be the highest, while an evaluation order of 20 will be the lowest.
   Note: The SNMP traps are mutually exclusive. If a value is detected by a trap, then the value will no longer be compared to any of the other traps that may exist. For example, you could create a catch-all trap with an evaluation order of 20 and other, more specific traps, with progressively higher evaluation orders to ensure other SNMP data is not missed by any of the other traps.
9. Once you have entered the appropriate information, click **Save**.

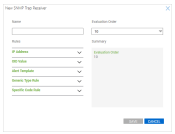
Sample Trap Creation

The Vertical Wave IP system sends traps in response to events taking place. For these traps, the value sent in the trap is the number of the trunk affected. The specific code sent in the header of the trap actually indicates what event has taken place. A subset of the traps, taken from Eventlog.mib, is shown below:

```
eventLog-VoiceMailDisksFull TRAP-TYPE
        ENTERPRISE  vertical
        VARIABLES {lastTrapLogType,
                                        lastTrapEventType,
                                        lastTrapInfoString }

        DESCRIPTION
" This notification is sent when the Voice Mail
                disk capacity is reached."
        -- 57

eventLog-SystemDiskFull TRAP-TYPE
        ENTERPRISE  vertical
        VARIABLES {lastTrapLogType,
                                        lastTrapEventType,
                                        lastTrapInfoString }

        DESCRIPTION
" This notification is sent when the specific
                disk capacity is reached."
        -- 58

eventLog-SecurityError TRAP-TYPE
        ENTERPRISE  vertical
        VARIABLES {lastTrapLogType,
                                        lastTrapEventType,
                                        lastTrapInfoString }

        DESCRIPTION
" This notification is sent when a failure audit
                event occurs, i.e. an audited access attempt fails.
                For example, a failed attempt to open a file is a
                failure audit event."
        -- 59

eventLog-SecuritySuccess TRAP-TYPE
        ENTERPRISE  vertical
        VARIABLES {lastTrapLogType,
                                        lastTrapEventType,
                                        lastTrapInfoString }

        DESCRIPTION
" This notification is sent when a success audit
                event occurs, i.e. when an audited access attempt
                is successful. For example, a successful logon
                attempt is a success audit event."
        -- 60
```

For this example, we want to capture when the voicemail disk is full (e.g., eventLog-VoiceMailDisksFull). According to the above example log, 57 is sent when the voice mail capacity has been reached.

1. From the **Network Probe** tile, click **SNMP Traps** on the navigation pane and then select the **SNMP Trap Receivers** tab .
2. Click on the **+** icon to add a trap.



3. Enter the **Name**. For our example, we will enter **Wave Device Voice Mail Full**.
4. Click on **Generic Type Filter** and then:
   a. Select **Equals** from the **Check Condition** drop-down.
   b. Enter **6** in the **Result** field. In most cases, you will use **6** when using the **Specific Code Filter**.
5. Click on **Specific Code Filter** and then:
   a. Select **Equals** from the **Check Condition** drop-down.
   b. Enter **57** in the **Result** field.
      Note: Given those other devices may use code 57, some additional filtering is probably a good idea. You could filter on IP address or if you know the trap OID, you can use this. For the current example, the Wave device OID is constant for all traps sent so that can be used.
6. If necessary, you may change the **Evaluation Order** from the default of **10** according to your needs.
7. Click on **OID Value Filter** to expand the list.
   a. Select **Any Thing** from the **Check Condition** drop-down.
   b. Leave the **Result** field empty.
8. Click **Save**. This will create a trap to receive messages when the voicemail is full based on the information provided in the Eventlog.mib.