SNMP Traps Screen in the Control Center

Overview

An SNMP trap is a message that is initiated by a network device and sent to the probe. For example, a router could send a message if one of its power supplies fail or a printer could send an SNMP trap when it is out of paper.

The purpose of SNMP Trap Filters is to allow you to set filters to define which traps should be accepted and which are thrown out. A trap has to pass a filter in order for it to be sent to the server. This allows devices to notify the probe of abnormal conditions. A Trap operation is different than the Get, GetNext and Set operations because it is initiated from a managed device. A trap message is used to alert to the fact that a specific threshold has been reached, or that an error or event of some type has occurred.

Devices must be configured to send SNMP traps to the probe-enabled computer. To enable and configure traps, review the specific device's documentation. Exclusive use of traps is not recommended for the following reasons:

- Traps only report some of the issues that indicate there is a problem with the device. For example, a device that has no power obviously cannot send a trap indicating power loss, but a constant network monitor will detect this issue.
- SNMP traps use the UDP protocol, which is not guaranteed to be received by the SNMP trap listener. SNMP traps are typically not rebroadcasted.

The SNMP Traps screen consists of two different tabs:

- SNMP Traps Received Tab
- SNMP Trap Receivers Tab

SNMP Versions

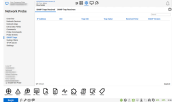
There are three versions of SNMP:

- Version 1 was the first version of SNMP. This is the most commonly used version. The major drawbacks with version 1 are no support for 64-bit numbers and poor security.
- Version 2 initially provided support for 64-bit numbers, as well as an enhanced security model. However, the version 2 security model is not widely accepted. Because of this, there are multiple standards of Version 2, the most commonly used being Version 2vc. This is the version supported by ConnectWise Automate®. Version 2 is used mostly by high-speed routers and switches to count incoming/outgoing bytes.
- Version 3 provides encryption (scrambling of the message so it is not viewable across the network) and authentication (verification that the SNMP message actually came from the device in question, and was not tampered with)

Versions 1 and 2 use an access keyword, referred to as the Community Name (or Community String), as a simple form of security. However, this method is not secure due to the fact the community name is simply placed in the header of the message, and thus visible to anyone monitoring the network. Most modern devices have two community names, one that provides read-only access to the device (the public community name), and a private one that allows writing to certain objects.

SNMP Traps Screen Breakdown

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.



5. Select either the **SNMP Traps Received** tab or **SNMP Trap Receivers** tab.