APC Managed Services Integration Kit

APC Smart-UPS® and Kaseya® RMM Integration

Installation and Configuration Guide

990-9899A

12/2016

by Schneider Electric

Schneider Electric IT Corporation Legal Disclaimer

The information presented in this manual is not warranted by the Schneider Electric IT Corporation to be authoritative, error free, or complete. This publication is not meant to be a substitute for a detailed operational and site specific development plan. Therefore, Schneider Electric IT Corporation assumes no liability for damages, violations of codes, improper installation, system failures, or any other problems that could arise based on the use of this Publication.

The information contained in this Publication is provided as is and has been prepared solely for the purpose of evaluating data center design and construction. This Publication has been compiled in good faith by Schneider Electric IT Corporation. However, no representation is made or warranty given, either express or implied, as to the completeness or accuracy of the information this Publication contains.

IN NO EVENT SHALL SCHNEIDER ELECTRIC IT CORPORATION, OR ANY PARENT, AFFILIATE OR SUBSIDIARY COMPANY OF SCHNEIDER ELECTRIC IT CORPORATION OR THEIR RESPECTIVE OFFICERS, DIRECTORS, OR EMPLOYEES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, CONTRACT, REVENUE, DATA, INFORMATION, OR BUSINESS INTERRUPTION) RESULTING FROM, ARISING OUT, OR IN CONNECTION WITH THE USE OF, OR INABILITY TO USE THIS PUBLICATION OR THE CONTENT, EVEN IF SCHNEIDER ELECTRIC IT CORPORATION HAS BEEN EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SCHNEIDER ELECTRIC IT CORPORATION RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES WITH RESPECT TO OR IN THE CONTENT OF THE PUBLICATION OR THE FORMAT THEREOF AT ANY TIME WITHOUT NOTICE.

Table of Contents

Preliminary Information

Introduction

APC Managed Services Integration Kits provide advanced SNMP monitoring of APC Smart-UPS® with Remote Monitoring and Management (RMM) solutions, using integrated SNMP Monitor Sets. This document details the process to configure SNMP polling and traps for APC Smart-UPS, using the Kaseya® Remote Monitoring and Management (RMM) solutions. The SNMP Object Identifiers (OIDs) and traps detailed allow Managed Service Providers to monitor APC Smart-UPS with a Network Management Card (NMC) AP9630, AP9631 or AP9635 installed.

System Requirements

To configure Kaseya for SNMP Monitoring of APC Smart-UPS, the following configuration is required:

- Kaseya Virtual System Administrator (VSA) version 9.3 or higher.
  - See **Kaseya System Requirements** available on the Kaseya VSA Online help (**help.kaseya.com**) for specific operating system and browser requirements.
  - For Kaseya VSA technical support, visit **Kaseya Customer Support.**
- APC Smart-UPS with an NMC 2 installed. See “Supported Devices”.
  - SNMPv1 is supported by the **Monitor** module in Kaseya VSA. See “Monitoring with the Kaseya Monitor Module” on page 2.
- Monitoring with SNMPv3 is not supported.

Supported Devices

Advanced SNMP monitoring of APC Smart-UPS with Kaseya RMM using an integrated SNMP monitor set is available for APC Smart-UPS with a Network Management Card 2 installed (AP9630, AP9631 and AP9635).

Related Documents

The APC by Schneider Electric website, **www.apc.com**, includes the following UPS Network Management Card documentation:

- **Network Management Card 2 Installation Guide**, for AP9630, AP9631, and AP9635. See the NMC 2 Installation Guide for detailed instructions on the installation and configuration of the Network Management card for APC Smart-UPS.
- **Network Management Card 2 User Guide**, for AP9630, AP9631, and AP9635. See the NMC 2 User Guide for detailed network and SNMP configuration of the Network Management Card 2.

Monitoring with the Kaseya Monitor Module

The Kaseya Monitor Module supports monitoring of APC Smart-UPS devices with SNMPv1.

Terminology

SNMP Monitor Set
A collection of OIDs and descriptions that can be assigned to one or more SNMP-enabled devices**.**

SNMP Traps Alert
When an Agent Procedure is run on a Kaseya managed machine, a service called `Kaseya SNMP Trap Handler` is started on that machine that listens for SNMP trap messages sent by SNMP-enabled devices. Kaseya uses the System Process called `ksnmptrapd.exe` to receive and process the SNMP traps. This process logs the information into the operating system Event Log.

Probe Agent
A Kaseya managed machine that polls for SNMP data, and listens for SNMP Trap messages sent by SNMP-enabled devices. This machine is used by the Kaseya Discovery process to discover all SNMP-enabled devices on the network.

SNMP Trap Event Set
A collection of terms and source references to detect events and raise alarms, based on severity.

KaseyaSNMPTrapHandler
The System Process KSNMPTrapd.exe is invoked by the SNMP Trap Handler service.

Prerequisite Kaseya Discovery Process

The Kaseya Discovery Process finds all SNMP-enabled devices on the network. Run the discovery process through the Kaseya user interface by selecting:

Discovery > Networks > By Network

1. Click on the **New** icon to perform a new network scan.
2. On the **General** tab, enter:
    a. **Network Name**
    b. **Probe** - select a Kaseya Agent that communicates with the network during Discovery.
    c. **Organization**

    All other fields can remain blank.
3. On the **SNMP** tab, enable SNMP and enter the **Community String**. The Discovery network scan can only identify SNMP devices that share the same SNMP read Community String. Typically, the default read Community String value is `public`. Community strings are case sensitive.
4. Select **Save & Scan** to execute the scan.

For more information on the Kaseya Discovery Process, see the "*Discovery"* Online Help at **help.kaseya.com**.

Network Management Card SNMP Configuration

Once SNMP-enabled devices have been discovered by Kaseya on the network, the Network Management Cards available on the network can be configured to send the SNMP Trap alerts to the Kaseya Agent. For each Network Management Card on the network, open the **NMC Web interface** in a web browser.

SNMPv1 Configuration:

1. To confirm that SNMPv1 is enabled, go to **Configuration > Network > SNMPv1 > Access** and check that the **Enable** checkbox is selected. SNMPv1 is enabled by default.
2. Go to **Configuration > Notification > SNMP Traps > Trap Receivers** and click **Add Trap Receiver.**
3. Enter the Trap Receiver details of the **Probe Agent** used in the Kaseya Discovery Process. Enter:
   - **Trap Generation**: Enable
   - **NMS IP / Host Name**: Enter the IP Address of the Kaseya Probe Agent.
   - **Language**: Select desired language of SNMP Traps. English is the default.
   - **SNMPv1 Community Name**: Enter the Community String used in the Kaseya Discovery Process. The default string is `public`.
   - **Authenticate traps**: Enable.
4. Click **Apply** to save the Trap Receiver settings.

NOTE: To configure Kaseya to successfully receive an SNMP Trap, see “Start the SNMP Trap Handler” on page 8, “Verify the SNMP Trap Handler Service” on page 9 and “Configure the Probe Event Log Settings” on page 10.

5. To test the Trap Receiver settings, go to **Configuration > Notification > SNMP Traps > Test**. Select the Probe Agent Trap Receiver from the dropdown list and click **Apply.**
6. To verify that the Trap has been received, open the Kaseya VSA interface and go to **Agent > Agents> Agent Logs > Event Logs**, select the Probe Agent and view the Application event logs.

SNMP Monitor Sets

Overview

The Kaseya SNMP Monitor Sets for APC Smart-UPS are available for download from the **APC by Schneider Electric** website, **www.apc.com**.

Inventory

The self-extracting executable contains ten files.

Four XML Polling Monitor Sets:

- **APC Smart UPS – About**
  The About Monitor Set provides information about the UPS such as Model, Part Number, Serial Number, Manufacture Date and Battery related information. See “SNMP About Information” on page 5.
- **APC Smart UPS – Config**
  The Config Monitor Set provides information about the configuration of the UPS, such as Alarm Status, Self Test Interval and Voltage Transfer points. See “SNMP Configuration Information” on page 5.
- **APC Smart UPS – Group Config**
  The Group Config Monitor Set provides information about the configuration of the UPS Outlet Groups,

such as Outlet Group Name, Outlet Group Index, and Power Off Delays. See “SNMP Outlet Group Information” on page 5.

- **APC Smart UPS – Status**
  The Status Monitor Set provides information about the status of the UPS, such as Battery Charged Percentage, Load, Battery Voltage, and Battery Temperature. See “SNMP Status Information” on page 5.

Three XML Trap Event Sets:

- **APC Smart UPS – Traps**:
  a. Informational
  b. Warning
  c. Severe

  The Trap Event Monitor Sets define a set of UPS events upon which SNMP Traps can be raised. The events are divided into three sets: Informational events, Warning events and Severe events. This allows for the configuration of appropriate notifications, based upon severity. See “SNMP Trap Events” on page 5.

Two Kaseya Agent Procedures:

- **Kaseya Agent Procedures**
  Included with the SNMP monitor sets are two Kaseya Agent Procedures for creating and removing the functionality for SNMP Trap Handling:
  - `Exec Inst KaseyaSNMPTrapHandler.xml`
  - `Exec Remove KaseyaSNMPTrapHandler.xml`

  See “View the SNMP Trap Event Logs” on page 10 for more information on how to use the Kaseya Agent Procedures.

One Trap Handler Monitor Set:

- **KaseyaSNMPTrapHandler Monitor Set**
  Also included is a Monitor Set to check if the KaseyaSNMPTrapHandler is running, which attempts to restart the service if it has stopped, and can notify in such an event:
  - `KaseyaSNMPTrapHandler Service Check.xml`

  See “Verify the SNMP Trap Handler Service” on page 9 for more information.

Object Identifiers (OIDs)

The table below lists the OID names made available in each Monitor Set. They provide APC Smart-UPS status and configuration information for SNMP polling, and SNMP trap alerts for key events.

SNMP About Information

- upsBasicIdentModel
- upsAdvIdentSkuNumber
- upsAdvIdentSerialNumber
- upsAdvIdentDateOfManufacture
- upsAdvBatteryInternalSKU
- upsAdvBatteryExternalSKU
- upsBasicBatteryLastReplaceDate
- upsAdvBatteryRecommendedReplaceDate
- upsAdvIdentFirmwareRevision

SNMP Configuration Information

- upsAdvConfigAlarm
- upsAdvConfigAlarmTimer
- upsAdvTestDiagnosticSchedule
- upsAdvConfigLowTransferVolt
- upsAdvConfigHighTransferVolt
- upsAdvConfigLowBatteryRunTime
- upsBasicStateOutputState

SNMP Outlet Group Information

- upsOutletGroupConfigPowerOffDelay
- upsOutletGroupConfigPowerOnDelay
- upsOutletGroupStatusGroupState
- upsOutletGroupStatusName
- upsOutletGroupStatusIndex
- upsOutletGroupStatusTableSize

SNMP Status Information

- upsBasicStateOutputState
- upsHighPrecOutputLoad
- upsHighPrecBatteryCapacity
- upsAdvBatteryRunTimeRemaining
- upsHighPrecOutputCurrent
- upsHighPrecBatteryTemperature
- upsHighPrecOutputEfficiency
- upsHighPrecOutputEnergyUsage
- upsHighPrecBatteryActualVoltage
- upsHighPrecInputLineVoltage
- upsHighPrecInputFrequency
- upsHighPrecOutputVoltage
- upsHighPrecOutputFrequency
- upsAdvInputLineFailCause
- upsAdvTestDiagnosticsResults
- upsAdvStateAbnormalConditions

SNMP Trap Events

Informational

- apcInternalCommunicationFaultCleared
- batteryOverTemperatureCleared
- communicationEstablished
- noBatteriesCleared
- powerRestored
- returnFromBypass
- returnFromLowBattery
- smartAvrReducingOff
- upsBatteryReplaced
- upsCriticalConditionCleared
- upsDiagnosticsPassed
- upsInformationalCondition
- upsInformationalConditionCleared
- upsOutletGroupTurnedOn
- upsOverloadCleared
- upsTurnedOn
- upsWokeUp

Warning

- batteryOverTemperature
- noBatteries
- smartAvrReducing
- upsOutletGroupCommand
- upsOutletGroupTurnedOff
- upsSleeping
- upsTurnedOff
- upsWarningCondition
- upsWarningConditionCleared

Severe

- apcInternalCommunicationFault
- communicationLost
- hardwareFailureBypass
- lowBattery
- upsBatteryNeedsReplacement
- upsCriticalCondition
- upsDiagnosticsFailed
- upsOnBattery
- upsOverload

Installation

Prerequisites

In advance of SNMP Monitor Set installation in Kaseya, make sure that the following steps are complete:

1. The Kaseya Discovery process has discovered all SNMP-enabled devices on the network, and a **Probe Agent** has been defined. See “Prerequisite Kaseya Discovery Process” on page 2.
2. Download the PowerNet MIB file from **www.apc.com**. Rename the file to `powernetXXX-MIB.txt` where `XXX` is the version number of the PowerNet MIB, and save the file to the Probe Agent machine in the Kaseya Agent working directory (e.g. c:\kworking\usr\share\snmp\mibs)**.**
3. The Network Management Card Trap Receiver has been set to the IP address of the Probe Agent. See “Network Management Card SNMP Configuration” on page 3.
4. The SNMP Monitor Set files have been downloaded from the APC website. See “SNMP Monitor Sets” on page 3.

There are four steps in the process to add SNMP monitoring for APC Smart-UPS to Kaseya RMM:

1. Import the SNMP Polling Monitor Sets and SNMP Trap Event Sets to Kaseya. See “Import the SNMP Monitor Sets to Kaseya” on page 6 and “Configuring SNMP Traps” on page 8.
2. Assign the SNMP Monitor Sets to APC Smart-UPS devices on the network. See “Assign the SNMP Monitor Sets” on page 6.
3. Configure the Trap Handler and assign SNMP Trap Event Sets to the Trap Receiver of the RMM. See “Configuring SNMP Traps” on page 8 and “Configure the Probe Event Log Settings” on page 10.
4. Add thresholds to the SNMP Polling OIDs. See “Create a Monitor Threshold for SNMP Polling OIDs” on page 8.

Import the SNMP Monitor Sets to Kaseya

1. Download the SNMP Monitor Sets for APC Smart-UPS from **www.apc.com**. Save the files to your computer.
2. On the Kaseya **Monitor** Tab, select **Edit > SNMP Sets**. It is recommended to create a new folder entitled **APC Smart-UPS** under the **Shared** cabinet, and provide access via the **Share** icon.
3. Select the APC Smart-UPS folder created in step 2 and click **Import SNMP Monitor Sets** from top menu. Using the file explorer, navigate to the location of the Monitor Sets downloaded in step 1, and click the Upload button.

   NOTE: You can also paste the XML source of the Monitor Set files directly into the **Paste** area of the Import SNMP Monitor Sets dialog.

   Once the import is successful, you can assign the SNMP Monitor Sets to APC Smart-UPS devices that have been discovered by the Kaseya Probe Discovery. See “Prerequisite Kaseya Discovery Process” on page 2.

Assign the SNMP Monitor Sets

1. On the **Monitor** tab, navigate to **SNMP Monitoring > Assign SNMP**. Select the **Probe Agent** that was used in the “Prerequisite Kaseya Discovery Process”. A list of devices that are validated as SNMP-enabled is displayed.

2. Select one or more of the APC Smart-UPS in the list, then:
    a. Select one of the APC Smart UPS SNMP Monitor Sets from the dropdown list.
    b. Select one or more of the Action Types (Create Alarm, Create Ticket, Run Script and Email Recipients) to execute if an Alarm level defined in the SNMP Monitor Sets is triggered. See the “Create a Monitor Threshold for SNMP Polling OIDs” on page 8 for instructions on how to change Alarm levels.
    NOTE: Once an action is assigned to a Monitor Set, you can verify that the alarm is generated by viewing **Monitor > Status > Alarm Summary**, following a five minute interval.
3. Select **Add Monitor Set** to assign and append the monitor set to the device, or select **Replace Monitor Set(s)** to replace any monitor sets currently applied to the device. Click **Apply** to assign the SNMP Monitor Set.

Repeat steps 1-3 for the assignment of each “APC Smart-UPS” SNMP Monitor Set.

Verify Assignment

To verify that an SNMP Monitor Set assignment has been scheduled, hover the mouse pointer over the Kaseya Agent Status icon( ) and select the **Pending Procedures** (or **Procedure History** if Kaseya has already processed the request).

View SNMP Data Logs

To view SNMP data output of the SNMP polling run by the **Probe Agent,** select **Monitor Tab > SNMP Monitoring > SNMP Log**:

1. Select the **Probe Agent**.
2. Select the Device ID.
3. Click on the down arrow icon to display the value returned by the OID check. A bar chart or table is displayed at the bottom of the page.

Hover the mouse pointer on the abbreviated description to display the entire description. **NOTE:** The extended description is used to define the value returned via SNMP, as many of the APC OIDs are enumerated status codes.

See “Create a Monitor Threshold for SNMP Polling OIDs” on page 8 for more information on the description of values returned by an OID check.

To see more information on these values over time, you can generate and schedule reports through the Kaseya Report Center: **Info Center > Reporting > Reports**.

For more information on creating Kaseya Reports, see the *Info Center* chapter of the *VSA User Guide* at **help.kaseya.com**

Set up Outlet Group instances (multiple OID table entries)

Depending on the configuration of the UPS Master Outlet Groups (MOG) and Switched Outlet Groups (SOG), there may be multiple entries in the SNMP Log for the outlet groups. The index of the Outlet Group is based on the model and configuration of the UPS. To find out the **Number of Outlet Group Entries:**

1. Select **Monitor tab > SNMP Monitoring > Assign SNMP**
2. Select the Probe Agent.
3. Click on the device icon and click **Perform SNMPWalk**.
4. The Number of Outlet Group Entries is present in the results, at OID `1.3.6.1.4.1.318.1.1.1.12.3.1`

NOTE: The default Outlet Group SNMP Instance (also called index) is configured for a UPS with **three** outlet groups.

If your UPS has a different number of outlet groups, change the SNMP Instance (index) to reflect the number of Outlet Groups on your UPS:

1. Go to **Monitor Tab > Edit > SNMP Sets**
2. Select the **Group Config** Monitor Set and click **Edit SNMP Monitor Set**.
3. Select `upsOutletGroupStatusIndex` and click on the Edit icon
4. Enter the SNMP Instance value as a number range (e.g. 1-3) or as a list (e.g. 1,2,3).

When the SNMP Instance (Index) value is edited, it automatically re-deploys the changes to all devices with that assigned SNMP Monitor Set.

Create a Monitor Threshold for SNMP Polling OIDs

You can create threshold levels for the data returned by the SNMP Polling Monitor Sets, and indicate what actions are assigned to those thresholds.

1. Go to **Monitor Tab > Edit > SNMP Sets.** Select a monitor set, and click on the **Edit SNMP Monitor Set** menu item.
2. Click on the Edit icon next to the OID that you want to edit.
3. To find the definition of the values used to set a threshold for a particular Monitor Set, see the description field for the SNMP OID line item, and click **Next**.
4. Enter the Alarm Operator and Threshold Values.
   NOTE: Some thresholds are pre-populated with recommended values.
4. Kaseya SNMP Monitor Sets automatically deploy once changed. To verify, hover the mouse pointer over the Kaseya Agent Status icon( ) and select **Pending Procedures** to verify the SNMP Set and SNMP MIB file procedures are scheduled and executed. See “Assign the SNMP Monitor Sets” to configure alerts for Monitor Set threshold violations.

Configuring SNMP Traps

Start the SNMP Trap Handler

APC by Schneider Electric provides Kaseya Agent Procedures for creating and removing the functionality for SNMP Trap handling, `KaseyaSNMPTrapHandler`. The Agent Procedures are provided with the SNMP Monitor Sets, see “Inventory” on page 3.

1. To start the `SNMPTraphandler` on the Probe Agent, go to **Agent Procedures > Manage Procedures > Schedule / Create**. Select a folder in which to place the agent procedures.
2. Select **Import Folder/Procedure**.
3. Use the file explorer to navigate to `Exec Inst KaseyaSNMPTrapHandler.xml`
4. Repeat steps 1-3 for `Exec Remove KaseyaSNMPTrapHandler.xml`
5. Select `Exec Inst KaseyaSNMPTrapHandler.xml` agent procedure and select the Agent Probe Machine. Click **Run Now**.

Verify the SNMP Trap Handler Service

APC by Schneider Electric provides a Monitor Set to check if the `KaseyaSNMPTrapHandler` is running, and to restart the service if it stops. The Monitor Set is provided with the SNMP Monitor Sets, see “Inventory” on page 3.

To upload the Monitor Set to Kaseya:

1. In Kaseya, go to **Monitor > Edit > Monitor Sets**
2. Select or create a folder to place the Monitor Set.
3. Click **Import Monitor Sets.**
4. Use the file explorer to navigate to `KaseyaSNMPTrapHandler Service Check.xml.`
5. **Upload** the Monitor Set.

To assign SNMP Trap Handler Service monitoring to the Probe Agent:

1. In Kaseya, go to **Monitor > Agent Monitoring > Assign Monitoring**
2. Select the Probe Agent used in the “Prerequisite Kaseya Discovery Process”.
3. Select the `KaseyaSNMPTrapHandler Service Check` from the dropdown list of Monitor Sets.
4. Select the notification actions of Create Alarm, Create Ticket, Run Script or Email Recipients.
5. Click **Apply** to assign the Monitor Set to the **Probe Agent**.

Edit the Configuration File

To configure Kaseya VSA to receive SNMP traps, it is necessary to define the community name of the incoming traps:

1. On the Probe Agent machine, navigate to the Kaseya Agent working directory (e.g. c:**kworking\usr\bin**) and open the **snmptrapd.conf** file in a text editor.
2. Set `authCommunity` to the community name defined in “Network Management Card SNMP Configuration” on page 3, e.g. `authCommunity public`
3. Save **snmptrapd.conf**
4. Restart the SNMP Trap Handler:
   – Run s`ervices.msc`
   – Right-click on the `KaseyaSNMPTrapHandler` service and restart the service.

Notes on Firewall Configuration

An active firewall may restrict port activity. To ensure that SNMP Traps are received:

- Make sure that the executable file for `KaseyaSNMPTrapHandler` service is allowed in the Inbound Rules of the firewall.
- Add `KSNMPTrapD.exe` to the allowed list of the Inbound Rules of the firewall on any Kaseya Agents that are acting as SNMP Probes.

Configure the Probe Event Log Settings

To receive SNMP Traps sent by APC Smart-UPS devices, Kaseya VSA must first be configured to receive events from the Probe Agent machine's Application event log:

1. Go to **Agent > Agents > Event Log Settings**
2. Select the checkbox beside the **Probe** machine used in "Prerequisite Kaseya Discovery Process" on page 2.
3. For **Event Log Types**, select **Application**, and click **Add >>** to add it to the **Assigned Event Logs.**
4. Select **event categories**: **Error**, **Warning, Information**
5. Click **Update** to save the Probe Event Log assignment.

For more information on configuring Kaseya to receive events from the Probe Agent Application event log, see the *Monitor* > *SNMP Traps Alert* chapter of the *VSA User Guide* at **help.kaseya.com**

Import SNMP Event Sets

1. To import SNMP Event sets, select **Monitor Tab > Agent Monitoring > SNMP Traps Alert** and select the `<Import Event Set>` from the drop down list. Repeat this step for each Event Set: Severe, Warning and Informational.
   NOTE: If you experience browser issues importing the SNMP Event sets, use the latest Google® Chrome® browser.
2. Following successful import of the Event sets, a preview of the SNMP Trap Alert Set is displayed.
   NOTE: It may be necessary to refresh the page to view the updated SNMP Trap Alert Set.

Assign SNMP Trap Alert

The process to assign SNMP Trap Event Sets is similar to "Assign the SNMP Monitor Sets". There are three Trap Event Set types: Informational, Warning and Severe. You can set different actions per SNMP Trap type.

1. Go to **Monitor tab > Agent Monitoring > SNMP Traps Alert.**
2. Select the **Probe Agent** that was used in the "Prerequisite Kaseya Discovery Process".
3. Select one of the SNMP Trap Event Sets from the dropdown list entitled "Define events to match or ignore".
4. Select event categories, such as **Error**, **Warning, and Information**. The logs of some event categories (Success audit, Failure audit, Critical and Verbose) are not collected by Kaseya VSA, but alerts are still generated for those categories.
5. Specify the frequency of the alert condition required to trigger an alert.
6. Select the actions associated with the SNMP Trap Event: Create Alarm, Create Ticket, Run Script or Email Recipients.
7. Click **Apply** to assign the SNMP Trap Event Set to the Probe Agent.

NOTE: It may be necessary to refresh the page following each assignment to see the updated configuration.

View the SNMP Trap Event Logs

To verify that Traps are being captured in the Event log records:

1. Select **Agent > Agents > Agent Logs > Event Logs**
2. Select the **Probe Agent**.
3. Select the **Event Logs** tab. Once SNMP traps are received by Kaseya VSA, the Event Log displays them.

APC by Schneider Electric
Worldwide Customer Support

Customer support for this or any other APC by Schneider Electric product is available at no charge in any of the following ways:

- Visit the APC by Schneider Electric web site, www.apc.com to access documents in the APC Knowledge Base and to submit customer support requests.
  - **www.apc.com** (Corporate Headquarters)
    Connect to localized APC by Schneider Electric web site for specific countries, each of which provides customer support information.
  - **www.apc.com/support/**
    Global support searching APC Knowledge Base and using e-support.
- Contact the APC by Schneider Electric Customer Support Center by telephone or e-mail.
  - Local, country specific centers: go to **www.apc.com/support/contact** for contact information.
  - For information on how to obtain local customer support, contact the APC by Schneider Electric representative or other distributor from whom you purchased your APC by Schneider Electric product.

990-9899A 12/2016