APC™ Smart-UPS™ and ConnectWise® Automate™v10.5 RMM SNMP Integration

User Guide

990-9990

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

The APC Managed Services Integration provides advanced SNMP monitoring of APC Smart-UPS® with Remote Monitoring and Management (RMM) solutions, using integrated SNMP Monitoring. This user guide details the process to configure SNMP detection, monitors and traps for APC Smart-UPS, using the ConnectWise® Automate™ Remote Monitoring and Management (RMM) solution. 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 Automate™ for SNMP Monitoring of APC Smart-UPS, the following configuration is required:

- Automate™ RMM server version 10.5 or higher.
    - See **LabTech Installation Prerequisites** available on the Automate™ Documentation Portal (**docs.labtechsoftware.com**) for specific server and workstation requirements.
    - For Automate™ technical support, visit the Automate™ Partner Portal (**cp.labtechsoftware.com**).
- Any APC Smart-UPS with an NMC 2 installed. See Supported Devices.
    - SNMPv1 is supported to communicate between the APC device and the **Network Probe** in Automate™. See Monitoring with the Automate™ Network Probe.
- If PSA integration with Automate™ is desired, the ConnectWise® PSA plugin can be acquired from the Automate™ Solution Center.
    - For further information on the Automate™ Plugins and the Solution Center, see the Automate™ Documentation Portal.

Supported Devices

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

Prerequisites

APC

1) A Supported Device
2) Connected to an Internet Protocol (IP) network in which an Automate™ Computer is deployed and successfully checking into the Automate™ server.

Automate™

1) Automate™ 10.5 or higher
2) User credentials with Super Admin user permissions
3) Ability to access the Solution Center (remote or local to server)
4) The UPS Devices Solution from the Automate™ Solution Center

5) The latest APC PowerNet MIB loaded, see Add the APC PowerNet MIB to Automate™

Add the APC PowerNet MIB to Automate™

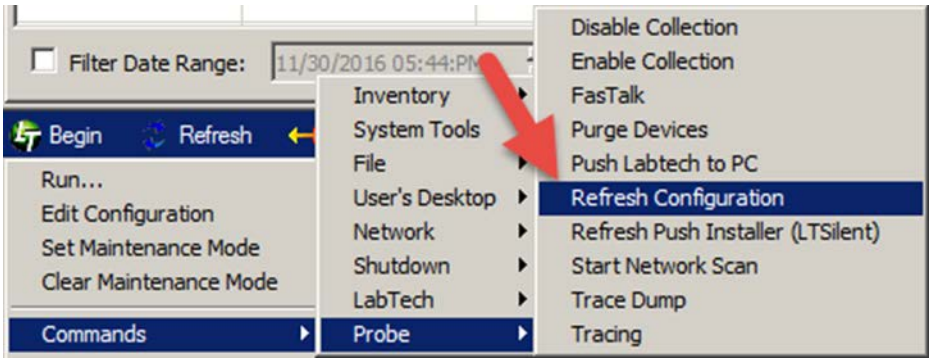
A MIB file helps identify what OIDs belong to what device and are valid to monitor.

1. Download the PowerNet MIB file
    a) Navigate to apc.com/tools/download
    b) On the Software/Firmware download page, click the drop down and select **Firmware Upgrades – MIB**
    c) Click **Submit**
    d) Find the latest version and click **Download**
        - **Note**: If the MIB file displays as text in a browser, right click on the page, click **Save as…** and if it saves it as a text file, change the file extension to **.mib** after saving it.
2. Load the MIB file
    a) Save/move the MIB file to C:\MIBS\RFC on the local machine where the Automate™ Control Center is installed.
        - The file can go in the LTShare\MIBs\RFC directory on the server if the Automate™ server is on the same network as the Automate™ Control Center being used for this configuration and the L drive is mapped correctly.
    b) Close the Automate™ Control Center, relaunch it, and then log back in.
    c) Open the Probe Template Management screen.
        - Click **Main > Probe Templates**
    d) On the Probe Template Management screen, click **Data > Reload MIB Files**
        - Wait a few moments for the MIB to reload; the Status screen will display when the MIBs complete loading.
    e) Add the MIB to the Automate™ database
        - From the Probe Template Management screen click, **Data > Store MIBs in LabTech**
        - If the option to purge the current list of OIDs in the database is presented, selecting **No** will maintain the current list of OIDs.

UPS Devices Solution

The UPS Devices Solution is obtained via the Automate™ Solution Center.

1. Login to the Automate™ Control Center with credentials that have Super Admin user permissions
2. Click **Tools > Solution Center**.
    - **Note:** The Solution Center may take a few moments to launch depending on how recently it has been accessed on the server and connection speed to it.
3. Add the UPS devices solution to the install queue
    a) Under the Solution Center navigation on the left click **Network Devices**.
    b) On the right-hand side find **UPS Devices** in the list of available solutions and click **Queue**.
        - **Note:** The status tag of **UPS Devices** solution may show as **New** or **Out of Sync**, either status is OK and will add or update the needed items in Automate™.
4. Click the **1 Solution in Queue** button
5. Click the **Install/Update** button
    - **Note:** It is recommended to check the box **Backup local database before update**.
6. Click **Yes** to the **Install/Update Notice**
7. Click **Finished**
8. Close the Solution Center
9. Refresh the Network Probe Configuration
    a) Open the Automate™ Network Probe
    b) Click **Begin > Commands > Probe > Refresh Config**



    c) Allow for the command to **Complete**. To check that the UPS Devices Solution has loaded successfully, view the **Probe Commands** tab.

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.

SNMP OID Reference Sheet

OID Name	OID
SNMP About Information	
upsBasicIdentModel	1.3.6.1.4.1.318.1.1.1.1.1.1
upsAdvIdentFirmwareRevision	1.3.6.1.4.1.318.1.1.1.1.2.1
upsAdvIdentDateOfManufacture	1.3.6.1.4.1.318.1.1.1.1.2.2
upsAdvIdentSerialNumber	1.3.6.1.4.1.318.1.1.1.1.2.3
upsAdvIdentSkuNumber	1.3.6.1.4.1.318.1.1.1.1.2.5
upsAdvBatteryInternalSKU	1.3.6.1.4.1.318.1.1.1.2.2.19
upsAdvBatteryExternalSKU	1.3.6.1.4.1.318.1.1.1.2.2.20
upsBasicBatteryLastReplaceDate	1.3.6.1.4.1.318.1.1.1.2.1.3
upsAdvBatteryRecommendedReplaceDate	1.3.6.1.4.1.318.1.1.1.2.2.21
SNMP Configuration Information	
upsAdvConfigHighTransferVolt	1.3.6.1.4.1.318.1.1.1.5.2.2
upsAdvConfigLowTransferVolt	1.3.6.1.4.1.318.1.1.1.5.2.3
upsAdvConfigAlarm	1.3.6.1.4.1.318.1.1.1.5.2.4
upsAdvConfigAlarmTimer	1.3.6.1.4.1.318.1.1.1.5.2.5
upsAdvConfigLowBatteryRunTime	1.3.6.1.4.1.318.1.1.1.5.2.8
upsAdvTestDiagnosticSchedule	1.3.6.1.4.1.318.1.1.1.7.2.1
upsBasicStateOutputState	1.3.6.1.4.1.318.1.1.1.11.1.1
SNMP Outlet Group Information	
upsOutletGroupStatusTableSize	1.3.6.1.4.1.318.1.1.1.12.1.1
upsOutletGroupStatusIndex	1.3.6.1.4.1.318.1.1.1.12.1.2.1.1
upsOutletGroupStatusName	1.3.6.1.4.1.318.1.1.1.12.1.2.1.2
upsOutletGroupStatusGroupState	1.3.6.1.4.1.318.1.1.1.12.1.2.1.3
upsOutletGroupConfigPowerOnDelay	1.3.6.1.4.1.318.1.1.1.12.2.2.1.3
upsOutletGroupConfigPowerOffDelay	1.3.6.1.4.1.318.1.1.1.12.2.2.1.4
SNMP Status Information	
upsAdvStateAbnormalConditions	1.3.6.1.4.1.318.1.1.1.11.2.1
upsAdvBatteryRunTimeRemaining	1.3.6.1.4.1.318.1.1.1.2.2.3
upsHighPrecBatteryCapacity	1.3.6.1.4.1.318.1.1.1.2.3.1
upsHighPrecBatteryTemperature	1.3.6.1.4.1.318.1.1.1.2.3.2

OID Name	OID
upsHighPrecBatteryActualVoltage	1.3.6.1.4.1.318.1.1.1.2.3.4
upsAdvInputLineFailCause	1.3.6.1.4.1.318.1.1.1.3.2.5
upsHighPrecInputLineVoltage	1.3.6.1.4.1.318.1.1.1.3.3.1
upsHighPrecInputFrequency	1.3.6.1.4.1.318.1.1.1.3.3.4
upsHighPrecOutputVoltage	1.3.6.1.4.1.318.1.1.1.4.3.1
upsHighPrecOutputFrequency	1.3.6.1.4.1.318.1.1.1.4.3.2
upsHighPrecOutputLoad	1.3.6.1.4.1.318.1.1.1.4.3.3
upsHighPrecOutputCurrent	1.3.6.1.4.1.318.1.1.1.4.3.4
upsHighPrecOutputEfficiency	1.3.6.1.4.1.318.1.1.1.4.3.5
upsHighPrecOutputEnergyUsage	1.3.6.1.4.1.318.1.1.1.4.3.6
upsAdvTestDiagnosticsResults	1.3.6.1.4.1.318.1.1.1.7.2.3

SNMP Trap Event Reference Sheet

Informational	Warning	Severe
apcInternalCommunicationFaultCleared	batteryOverTemperature	apcInternalCommunicationFault
batteryOverTemperatureCleared	noBatteries	communicationLost
communicationEstablished	smartAvrReducing	hardwareFailureBypass
noBatteriesCleared	upsOutletGroupCommand	lowBattery
powerRestored	upsOutletGroupTurnedOff	upsBatteryNeedsReplacement
returnFromBypass	upsSleeping	upsCriticalCondition
returnFromLowBattery	upsTurnedOff	upsDiagnosticsFailed
smartAvrReducingOff	upsWarningCondition	upsOnBattery
upsBatteryReplaced	upsWarningConditionCleared	upsOverload
upsCriticalConditionCleared		
upsDiagnosticsPassed		
upsInformationalCondition		
upsInformationalConditionCleared		
upsOutletGroupTurnedOn		
upsOverloadCleared	**Note:** Support for OIDs may vary between Smart-UPS models	
upsTurnedOn		
upsWokeUp		

Glossary

Definitions of commonly used words and terms in this documentation that may be foreign or context-sensitive.

Alert Template

Alert actions, contact information, start and end times and success and fail messages are configured in the **alert templates**. One **alert template** can be created to control the actions of hundreds of monitors. These actions can be set for time of day, and day of week, and can have multiple rules. For example, daytime alerts can perform different actions than night-time and weekend alerts.

Client

An Automate™ **Client** is a node in Automate™ used as a container to organize Locations with contain Computers. Clients are most readily accessed via the Automate™ Navigation Tree.

Computer

An Automate™ **Computer** is a node in Automate™ used as a container to organize information pertaining an individual computer with the Automate™ agent installed on it. Computers are sub-containers to Locations and multiple Computers may reside within a Location. Computers are most readily accessed via the Automate™ Navigation Tree.

Control Center

The Automate™ Control Center is the Automate™ client used by MSP technicians and engineers to remotely administer their connected computers.

Detection Template

An Automate™ SNMP **Detection Template** is a set of OIDs that the Network Probe uses to help detect information such as device Type, Manufacturer, Model, etc. on SNMP enabled devices, so they may be properly categorized in the Automate™ system. Detection templates get applied to devices by opening the **Network Probe** Computer then 1) Refreshing the Probe configuration by clicking **Begin > Commands > Probe > Refresh Config** and 2) under the **Settings** section click **Redetect Devices**. The device should then be listed in the **Network Devices** section on the **Network Probe** screen, click **Refresh** if it does not display immediately. To detect APC UPS Devices, use the unique identifier for APC devices in the detection template configuration. This identifier is always the first portion of the OID string, for APC it's 1.3.6.1.4.1.318.

Location

An Automate™ **Location** is a node in Automate™ used as a container to organize Computers. Locations are sub-containers to Clients and multiple Locations may reside within one Client. Locations are most readily accessed via the Automate™ Navigation Tree.

MIB

A management information base (**MIB**) is a formal description of a set of network objects that can be managed using SNMP. The format of the **MIB** is defined by the vendor and uses OIDs. The MIB file maps the OID to a known Module to provide further information about that OID.

Network Probe

An Automate™ **Network Probe** is a service running on a designated Automate™ agent computer per location that will scan the network for other devices without the Automate™ agent installed on them. It can be accessed via the **Automate™ Computer Management** screen **> Network Probe** tile.

OID

Object identifiers (**OID**s) are strings of numbers. They are allocated in a hierarchical manner, so that, for instance, the authority for "1.2.3" is the only one that can say what "1.2.3.4" means. With SNMP, it acts as an address to a precise stream that provides information about the device sending SNMP the packet(s).

Report Categories

Report Categories tie various monitors together into common categories to allow reporting on. They also provide data for various status gauges in Automate™.

Solution Center

The **Solution Center** is used to download updates and any new items that are available for the Automate™ system.

SNMP

SNMP is a protocol used for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, UPSs, switches, and routers on an Internet Protocol (IP) network. **SNMPv1** is the first version of SNMP and is the most widely version supported to date. It is the version that is supported in this integration document.

SNMP Community String

An **SNMP Community String** is like a password. It is sent along with each SNMP Get-Request and allows (or denies) access to device. Most network vendors ship their equipment with a default password of "public". (This is the so-called "default public community string".)

SNMP Trap

SNMP Traps enable an agent to notify the RMM application of significant events by way of an unsolicited SNMP message. The conditions to trigger a trap event from the UPS are defined in a Management Information Base (MIB) file loaded to the Automate™ server. After the condition has been met, the SNMP agent then generates an SNMP packet that is **sent** from the alerting device to the defined **receiving** SNMP Trap receiving device, the Automate™ Network Probe.

SNMP Walk

An **SNMP Walk** is an OID discovery run on a specific device to detect what SNMP OIDs respond and with what values in which Automate™ will then map the OID to the proper **MIB** module.

Detecting and Monitoring

Detecting and Monitoring APC Smart-UPS devices with the Automate™ Network Probe currently supports SNMPv1 only.

Enable Automate™ Network Probe Scan

The Automate™ Network Probe Scan finds all devices on the network and runs a detection process on all SNMP enabled devices. To perform a Network Probe Scan, follow these steps:

Enable the Network Probe

1. Follow the instructions available at **docs.labtechsoftware.com/LabTech10.5**
   In the documentation, see **Configuration > Network Probe > Enabling the Probe (Probe Wizard)**
2. For SNMP detection and monitoring with APC UPSs, pay attention to steps 9 and 12.
   a) Step 9, the default Community Strings should be fine but be certain “public,private” are, at minimum, included.
   b) Step 12, make sure that the box is checked to enable (default) “Collect Network Device Data for this Location”

Perform a Network Scan

1. From the **Clients** node, navigate to the **[Computer]** you wish to use as the probe and then double-click to open the **Computer Management** screen.
   - **Note:** The selected computer should be on the same LAN, VLAN and/or Subnet as the supported APC network device.
2. Select the **Network Probe** tab.
3. Click **Rescan Network** 

   - **Note:** This will trigger a scan of the network which takes on average about 5 to 15 minutes which allows for the time needed to perform further configuration steps.

SNMP Configuration

In order to receive SNMP data to monitor in Automate™, the Network Probe must be configured to receive SNMP Traps and the APC Network Management Cards must be configured to send SNMP Trap alerts to the Automate™ Network Probe Agent in the same Automate™ Location and on the same network.

Automate™ Network Probe

Detect the device and create an SNMP Trap Receiver.

Detect Devices

Detect and identify the device you want to monitor.

1. Open the Automate™ Network Probe
2. Under the **Settings** section click **Redetect Devices**
   a) Wait for the command to finish
3. From the **Navigation Tree**, find the desired **Location** > expand **Network** and find the desired UPS
   a) Click **Refresh** if the UPS does not immediately appear.

b) If the UPS continues to not show in the **Network Device** list, try and Perform a Network Scan again, wait 15 to 30 minutes and try to **Redetect Devices** again.

Create SNMP Trap Receiver(s)

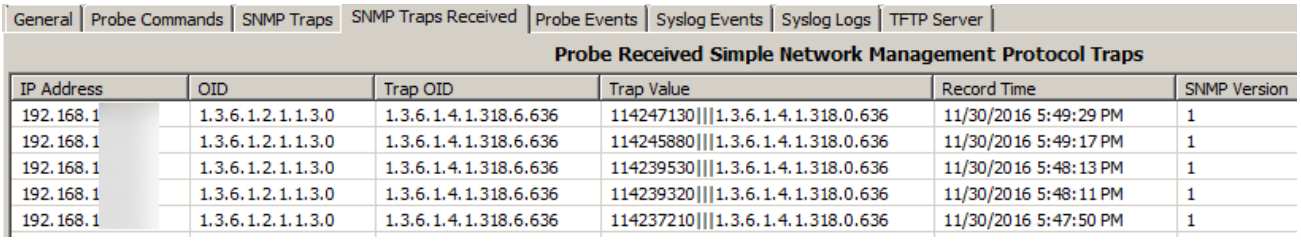
Once the desired UPS is identified, the SNMP Trap can be configured with the IP address.

1. Click **SNMP Traps**
2. Right click and click **Add Trap** to add a new SNMP Trap Receiver
3. 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. For the purpose of this integration we will just use the **IP Address** field.
4. An individual IP, comma separated list of IPs, a range of IPs or an entire subnet can be added. Below are some examples:
    a) A range of IP addresses between 10.45.6.70 and 10.45.6.90, inclusive. Enter in the following format, 10.45.6.[70-90].
    b) Every IP on a /24 subnet. Enter in the following format, 10.45.6.*
    c) Comma separated list. Enter the following format, 10.30.56.90, 10.30.56,95, 10.30.56.122 10.30.56.90, 10.30.56,95, 10.30.56.122
    d) Alternative way to 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].
5. The default **Evaluation Order** of 10 should be fine unless the **Network Probe** has been specifically configured to use other Evaluation Orders.
6. Click **Save**

APC Network Management Card

1. For each Network Management Card on the network, open the **NMC Web interface** in a web browser.
2. 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.
3. Go to **Configuration > Notification > SNMP Traps > Trap Receivers** and click **Add Trap Receiver.**
4. Enter the Trap Receiver details for the **Automate™ Network Probe Agent**.
    - **Trap Generation**: Enable
    - **NMS IP / Host Name**: Enter the IP Address of the Automate™ Network Probe Agent.
    - **Language**: Select desired language of SNMP Traps. English is the default.
    - **SNMPv1 Community Name**: Enter the Community String used during Enable the Network Probe. The default string is public.
    - **Authenticate traps**: Enable.
5. Click **Apply** to save the Trap Receiver settings.
6. 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.**

7. To verify that the Trap has been received, open the Automate™ Network Probe tab and go to **SNMP Traps Received**.



General | Probe Commands | SNMP Traps | SNMP Traps Received | Probe Events | Syslog Events | Syslog Logs | TFTP Server

Probe Received Simple Network Management Protocol Traps

IP Address	OID	Trap OID	Trap Value	Record Time	SNMP Version
192.168.1	1.3.6.1.2.1.1.3.0	1.3.6.1.4.1.318.6.636	114247130|||1.3.6.1.4.1.318.0.636	11/30/2016 5:49:29 PM	1
192.168.1	1.3.6.1.2.1.1.3.0	1.3.6.1.4.1.318.6.636	114245880|||1.3.6.1.4.1.318.0.636	11/30/2016 5:49:17 PM	1
192.168.1	1.3.6.1.2.1.1.3.0	1.3.6.1.4.1.318.6.636	114239530|||1.3.6.1.4.1.318.0.636	11/30/2016 5:48:13 PM	1
192.168.1	1.3.6.1.2.1.1.3.0	1.3.6.1.4.1.318.6.636	114239320|||1.3.6.1.4.1.318.0.636	11/30/2016 5:48:11 PM	1
192.168.1	1.3.6.1.2.1.1.3.0	1.3.6.1.4.1.318.6.636	114237210|||1.3.6.1.4.1.318.0.636	11/30/2016 5:47:50 PM	1

   - If you don't see the test trap immediately, click **Refresh** and/or try searching the list for the expected UPS IP. It may take 15-30 minutes before this initial test works.

Creating Monitors

Now that the device(s) can now be detected and identified, adding monitors is the next step. There are a couple of ways to add monitors, 1) using pre-defined monitors or 2) creating from an SNMP Walk.

Pre-defined Monitors

Pre-defined monitors allow a quick way to add a monitor to an individual device or a group of devices.

Individual Device

A monitor on an individual device will monitor that device only.

1. From the **Navigation Tree**, find the desired **Location >** expand **Network**
2. Find the APC UPS device to create the monitor(s) on and double click it
3. Click the **Monitors** tab
4. Right click anywhere in the data grid and click **Add New Monitor**
5. On the **Location** tab
   a) Define a name for the monitor, and use the remaining default settings.
      - **Note:** It's good to have a naming convention that is universally identifies the alert and UPS related to this monitor. Example: **UPS - apcF2508D - Battery Status** which translates as *MonitorType – UPSName – CheckType*
6. On the **Alerting** tab
   a) Assign the desired **Alert Template**
      - **Note:** For the purpose of this integration document use the **Default – Create Ticket** Alert Template
7. On the **Configuration** tab
   a) Set the **Monitor Type** to **SNMP OID Check**
   b) Under **Preloaded SNMP Checks** choose:
      - Group: **UPS**
      - Manufacturer: **APC**
      - Model: **SmartUPS**
      - Check: Choose whichever item you would like to alert on from the dropdown list.
   c) The defaults for **Condition** and **Result** are fine but can be changed, if desired.
8. On the **Trending** tab
   a) All defaults are fine, unless otherwise desired by an administrator.

Network Device Group

A monitor applied to a network device group will automatically apply to all the devices joined to that group. This helps prevent from having to create repetitious monitors per individual device.

1. Login to the Automate™ Control Center
2. Via the Navigation Tree, navigate to the Group **Network Devices > UPS Devices > APC UPS > Smart-UPS** and double click on it to edit it.
3. Click on the **Network Devices** tab
    a) The UPS(s) should be listed in the data grid on the **Members List** tab
4. Click the **Monitors** sub-tab
5. Click the **Add** button
    a) On the **Create Network Device Monitor** wizard select:
        - **SNMP – Simple Network Management Protocol** and click **Next**
    b) Under **Known SNMP Checks** select:
        - Group: **UPS**
        - Manufacturer: **APC**
        - Model: **SmartUPS**
        - Check: Choose whichever item you would like to alert on from the dropdown list.
        - Click **Next**
    c) **Monitor Interval**
        - This should remain at a reason interval between 2-5 minutes to allow for accuracy but to also to help avoid using too many resources on the Network Probe computer.
    d) **Result Evaluation**
        - The group **Create Network Device Monitor** wizard does not pull in the default values for the results, please see the OID Reference Sheet in this document to apply the proper **Check** and **Result** values.
    e) **Configure Alerting**
        - When to Alert: **Every Time**
        - Alert Template: **Default – Create Ticket**
        - Ticket Category: **<Not Specified>**. If advanced ticketing and/or PSA integration is desired, a custom ticket category can be assigned. For example: **UPS**
        - Report Category: <Not Specified>. Optionally, something like SNMP Checks can be selected for instance and it will then be accounted for as an SNMP Check on certain built-in reports or any custom report pointing to that data. Also, custom Report Categories can be created and used, if desired.

From an SNMP Walk

An SNMP Walk offers the widest select of OIDs to choose from. When the monitor is created, it applies to the individual device.

1. Open the APC UPS Network Device from the Network Probe or the Network Navigation Tree
2. Click the **SNMP Explorer** tab
3. Click **Walk**
    - Use the Default values (empty and greyed out) to walk the device against all known OIDs. **Note:** This may take a longer amount of time to finish. Click **Send Command**.
    - To walk the device for only APC products, check the **Starting OID** box and enter the OID 1.3.6.1.4.1.318 in the text box and click **Send Command**.
4. When the walk completes, it will display a list of all known OIDs
    - **Tip:** To help with ease of navigating the OIDs follow these steps.

a) Set the **Display Options** *View As:* to **Tree**
b) Click the Minus icon  in the upper right corner next to **Result Count**
c) This will shrink all the results and allow expansion one level at a time.

5. Navigate to a desired OID to monitor
6. Rick click on the OID and click **Create Monitor**
7. On the Monitor creation screen
    - Click the **Location** tab and verify the **Monitor Name** is as desired
    - Click the **Alerting** tab
        a) Alert Template: **Default – Create Ticket**
        b) Alert Style: **Once**
        c) Alert Message: Default is fine, advance options are fine too.
        d) Ticket Category: **<Not Specified>**. If advanced ticketing and/or PSA integration is desired a custom ticket category can be assigned. For example: **UPS**
        e) Report Category: **<Not Specified>**. Optionally, something like **SNMP Checks** can be selected for instance and it will then be accounted for as an SNMP Check on certain built-in reports or any custom report pointing to that data. Also, custom Report Categories can be created and used, if desired.
    - Click the **Configuration** tab
        a) Use the defaults. **Condition** and **Result** as they may be adjusted as desired.
    - Click **Save**
    - The monitor will now be applied to the device it was created on and can be access via the **Monitors** tab on the Network Device.

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.