



Network Integrity Systems
1937 Tate Blvd. SE
Hickory, NC 28602
Phone: 828.322.2181
Fax: 828.322.5294

info@networkintegritysystems.com
www.networkintegritysystems.com

We Bring Security To Light™

Application Note: Deactivating Switch/Router Ports in Response to Intrusion Events

Each Interceptor channel has an optical switch that can block traffic flow in response to intrusion events. In extrinsic configurations, where there are several unmonitored fibers alongside a monitored fiber, and the Interceptor cannot block traffic flow when there is an intrusion event. One way to solve this problem is to have the Network Management Application react to Interceptor intrusion events by sending interface-down commands to the switches or routers that use the unmonitored fibers. In this manner, multiple fibers can be blocked in response to an Intrusion event on a single monitored fiber.

This application note will explain how to automatically turn switch and router interfaces off in response to intrusion events from an Interceptor. The program "What's Up Gold" is used in this app note, although the technique is not limited to that program. It is assumed that What's Up Gold has already been configured to monitor the Interceptor as described in application note "NIS WUG appnote".

1 The IF-MIB

Most switches and routers support the SNMP IF-MIB, which provides information and control of all the interfaces on that device. The variable `ifAdminStatus` is a writable variable that allows interfaces to be turned on and off. The OID for `ifAdminStatus` is ...

`1.3.6.1.2.1.2.2.1.7.x`

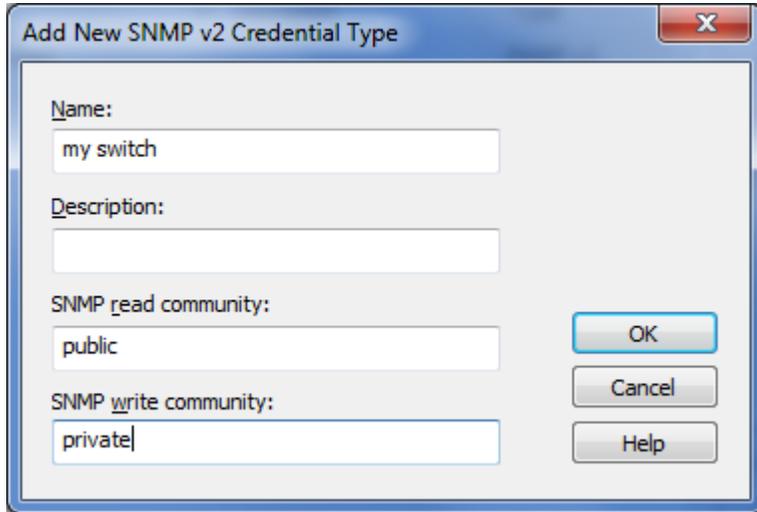
... where x is the interface number. The interface number normally matches the physical label on the device, but this may not be the case on complex devices.

`ifAdminStatus` is an integer with 1 meaning "up", and 2 meaning "down".

2 Add your switch

WUG must know about your switch to be able to control it. First, add an SNMP credential by clicking "Configure->Credentials...", then "New". The example below shows the creation of an SNMP v2 credential. SNMP v3 is preferred if your switch supports it.

We Bring Security To Light™



Add New SNMP v2 Credential Type

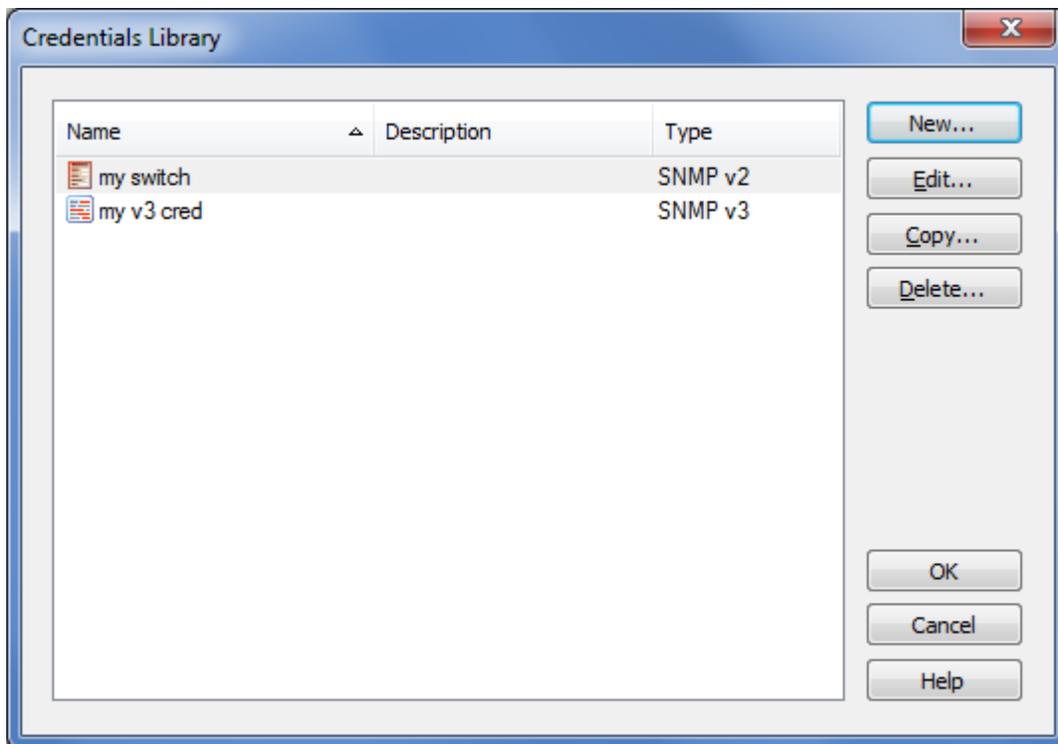
Name: my switch

Description:

SNMP_read community: public

SNMP_write community: private

OK
Cancel
Help



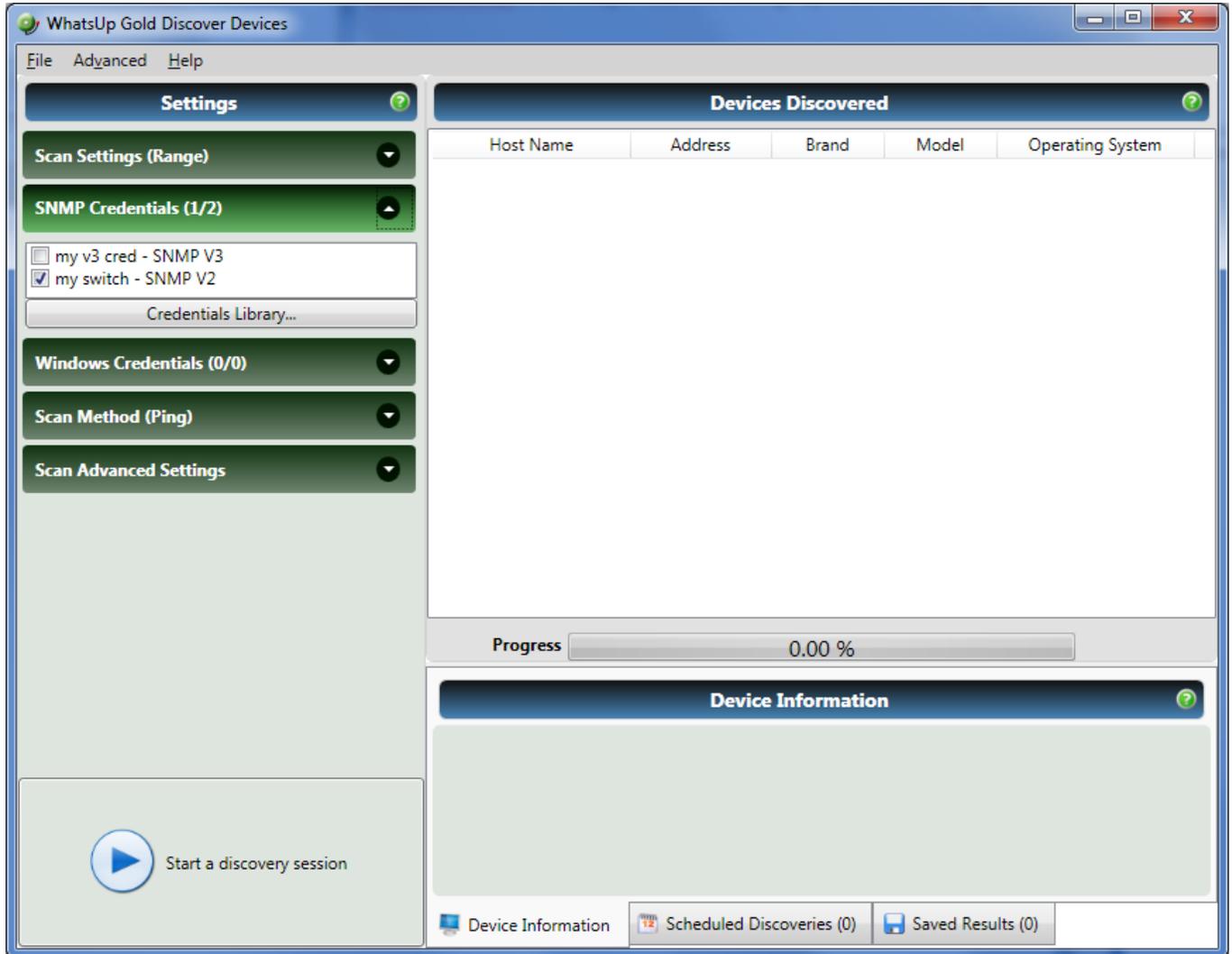
Credentials Library

Name	Description	Type
my switch		SNMP v2
my v3 cred		SNMP v3

New...
Edit...
Copy...
Delete...
OK
Cancel
Help

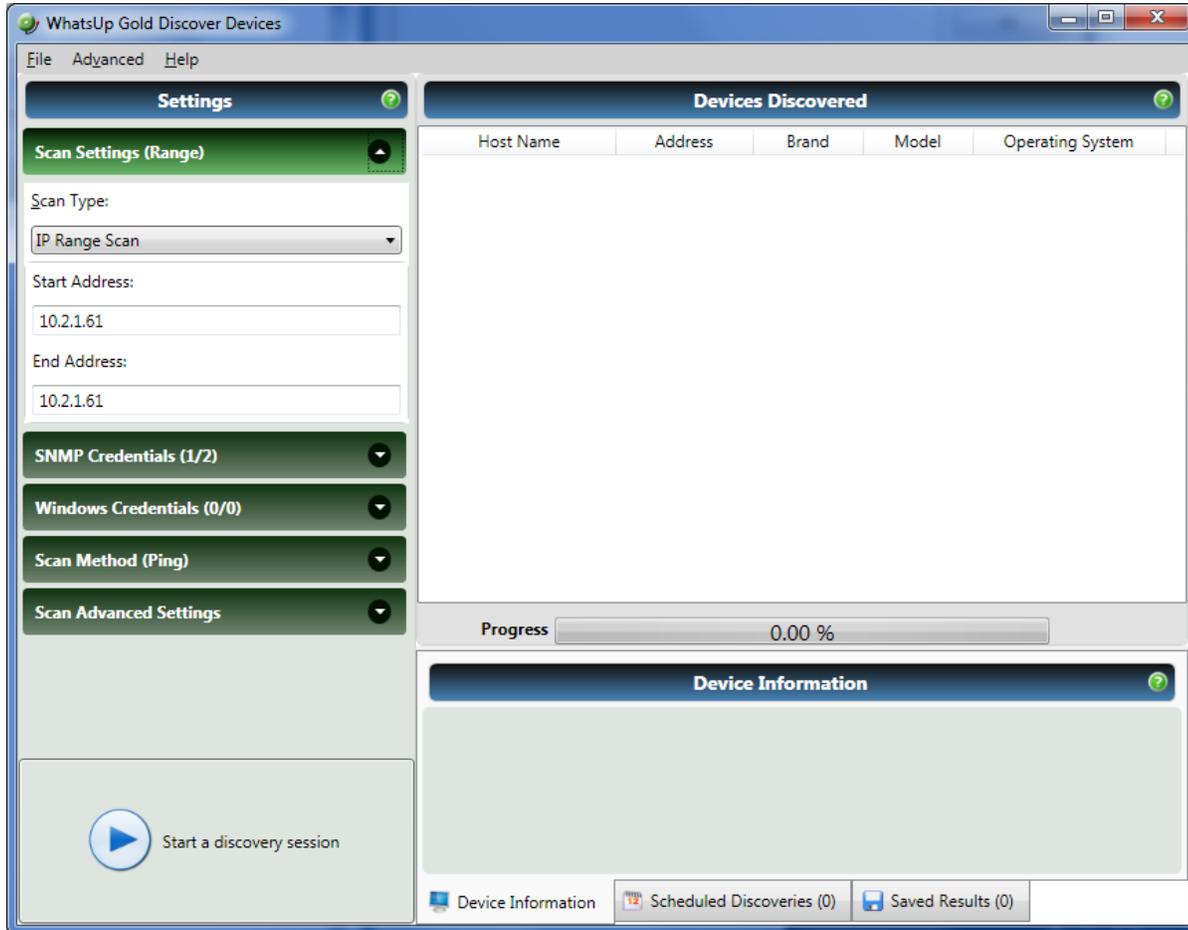
Next, get WUG to discover your device by clicking "Tools->Discover Devices...". Ensure your new SNMP credential is selected for the scan...

We Bring Security To Light™



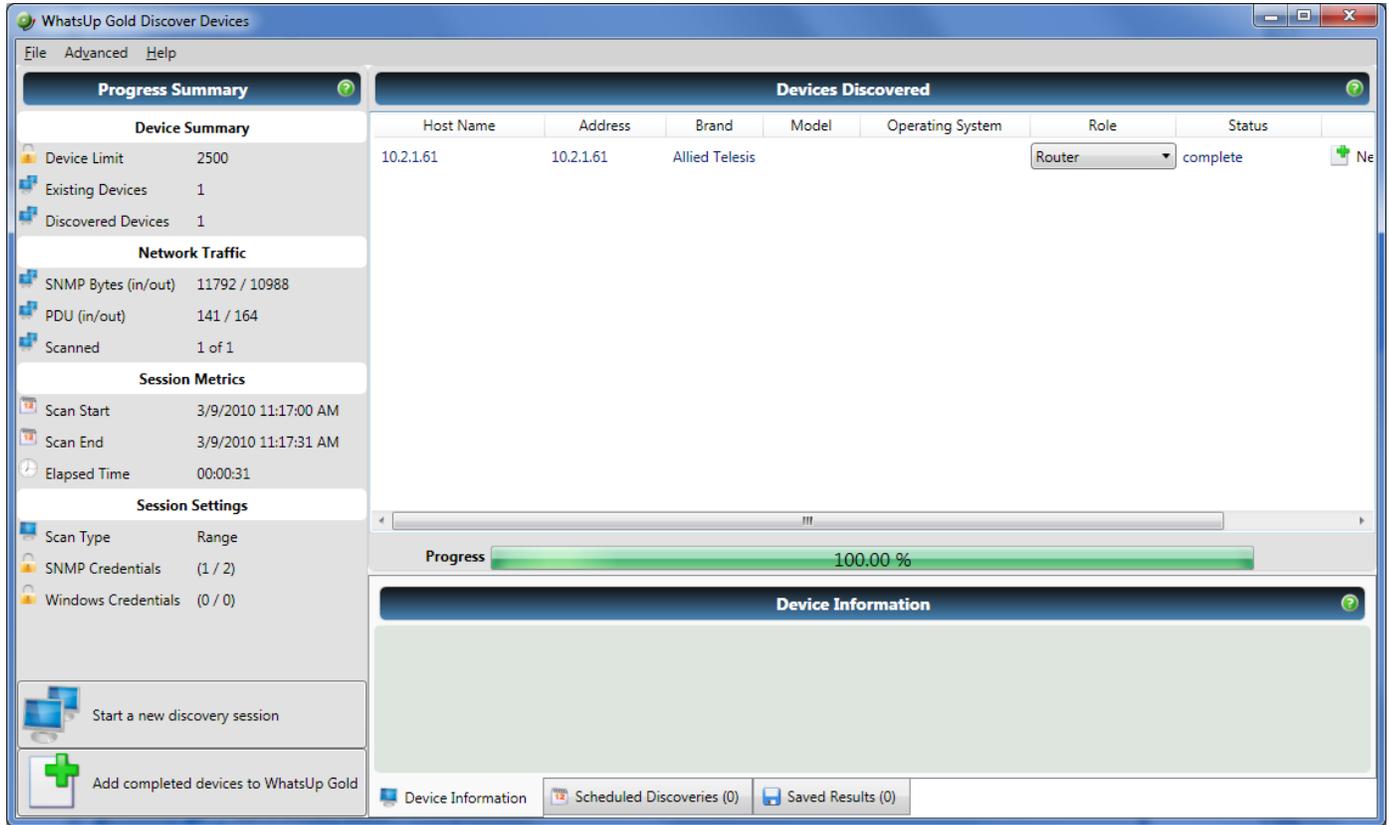
Adjust scan settings so that your switch will be detected...

We Bring Security To Light™



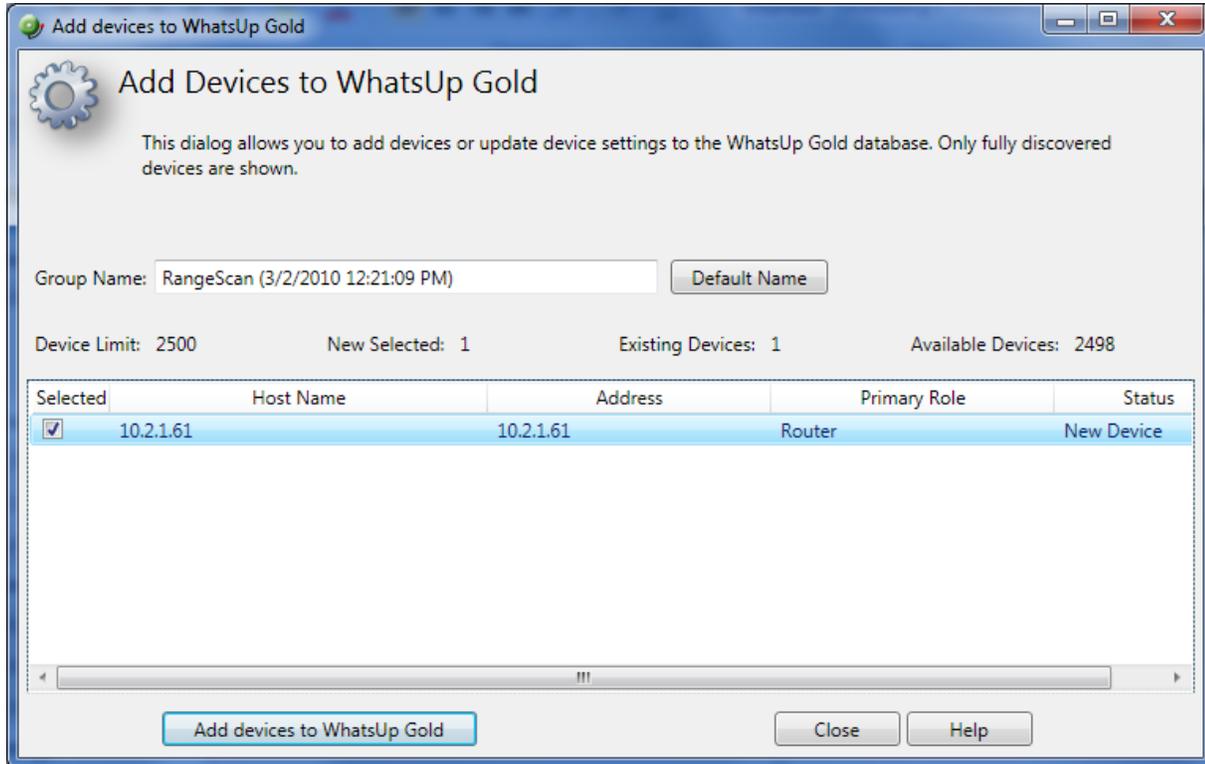
Click "Start a discovery session" to discover your switch...

We Bring Security To Light™



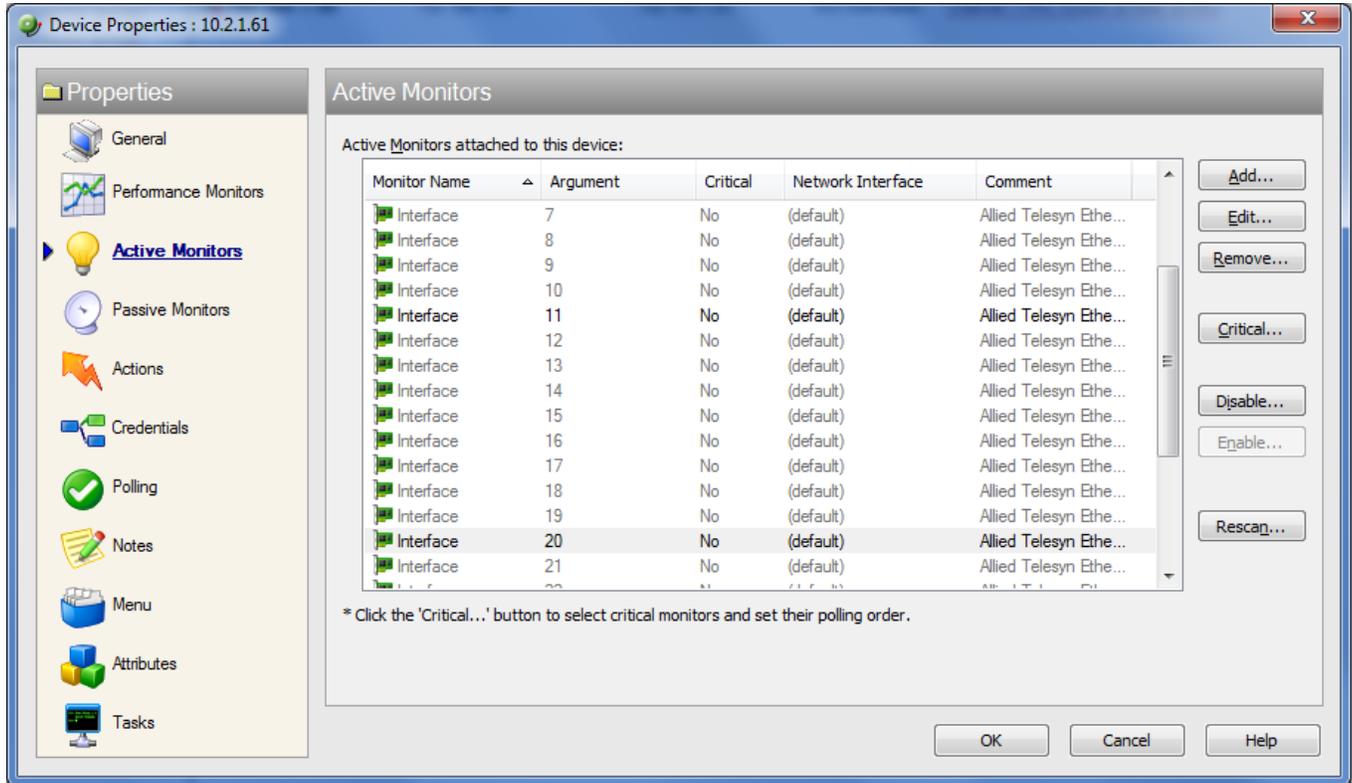
After this finishes, click "Add completed devices to WhatsUp Gold"...

We Bring Security To Light™



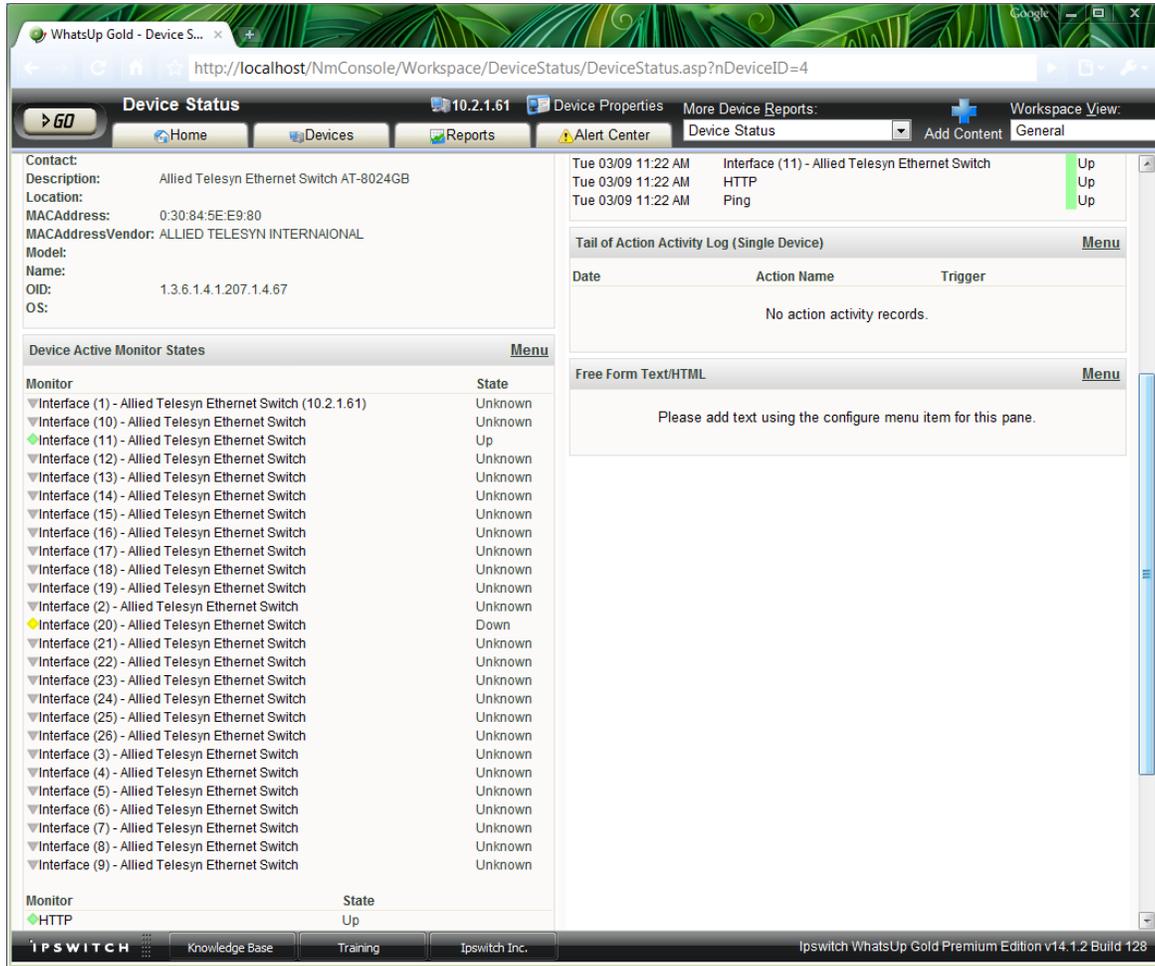
Select the switch, and click "Add devices to WhatsUp Gold". The switch will now have an Active Monitor for every interface in the switch. By default, monitors for interfaces that were down at detection time will be disabled. Double click on the device and click on "Active Monitors" to enable the monitors you need...

We Bring Security To Light™



View the switch through the WUG web interface to confirm that it is being monitored properly...

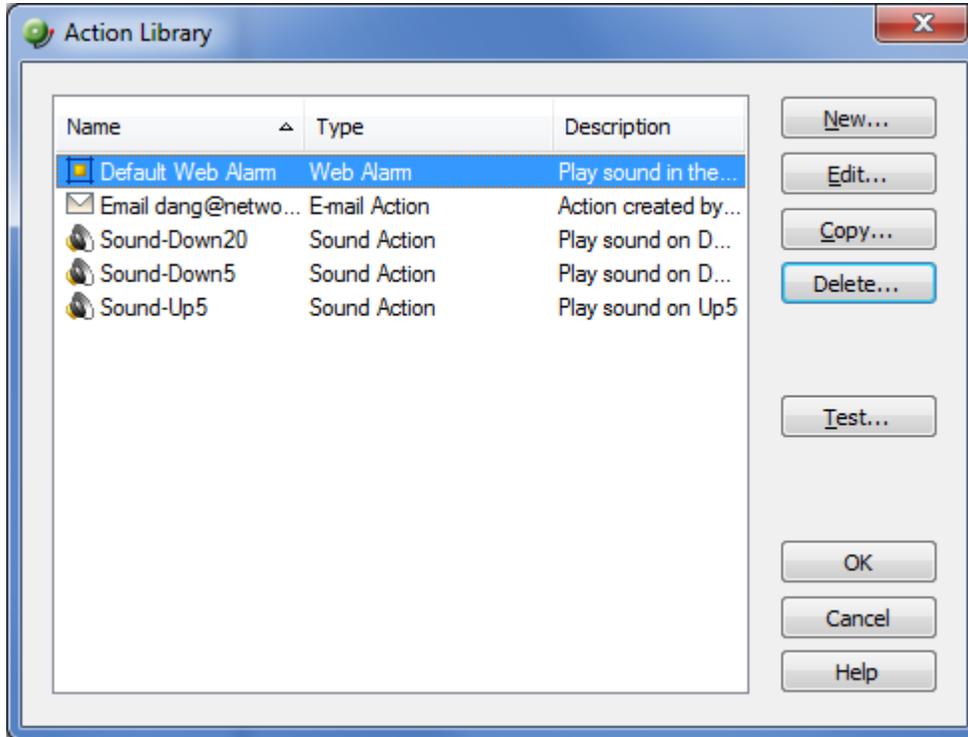
We Bring Security To Light™



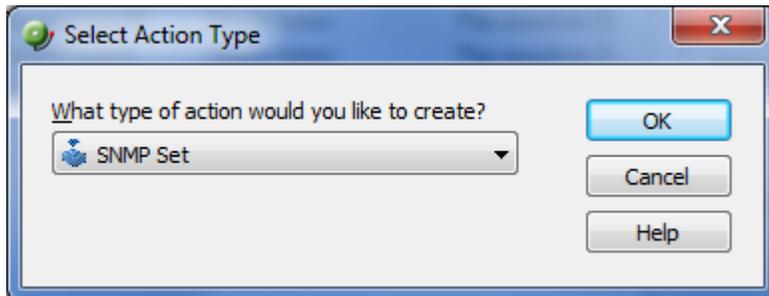
3 Add IF up/down actions

Now we will add Actions to bring interfaces up and down. For this example, we will add actions to control interface 20. Click "Configure->Action Library..."

We Bring Security To Light™

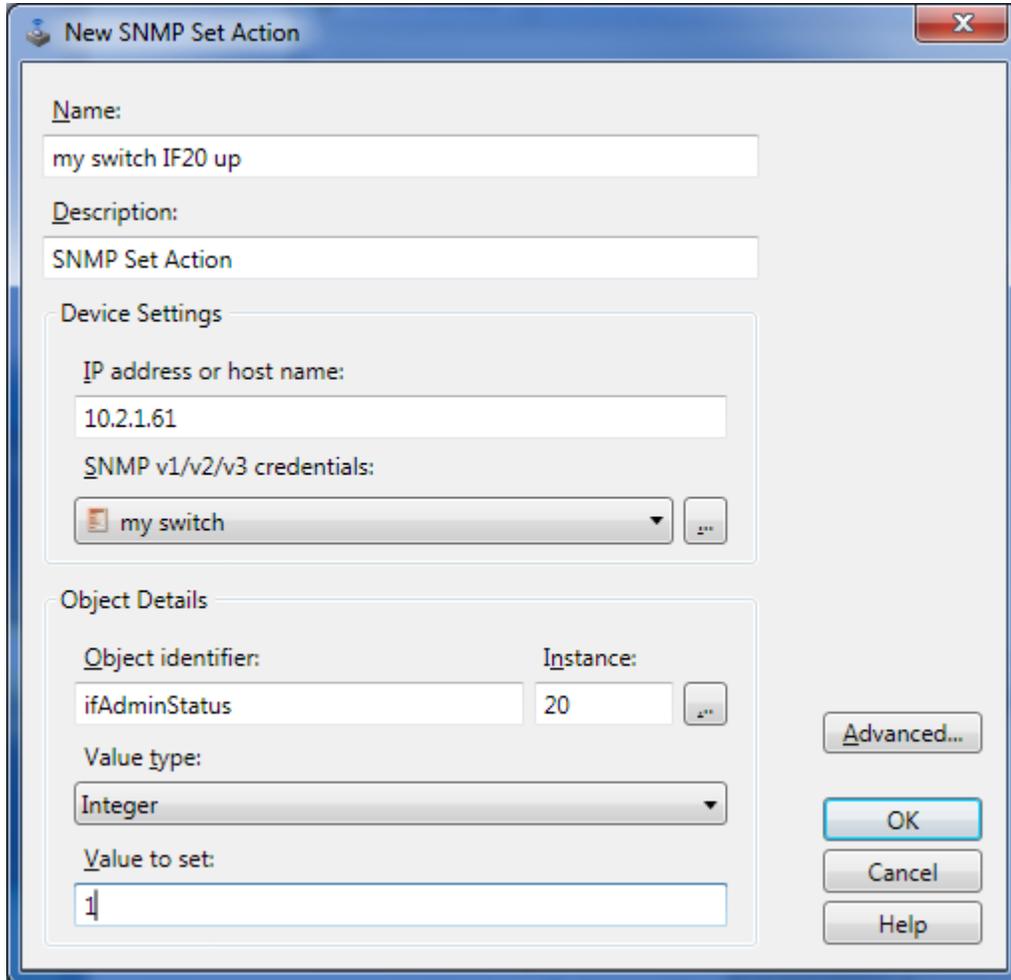


Click "New" and select SNMP Set...



Fill in the form as follows. Ensure you use your own values for IP address, SNMP credential, and Instance.

We Bring Security To Light™



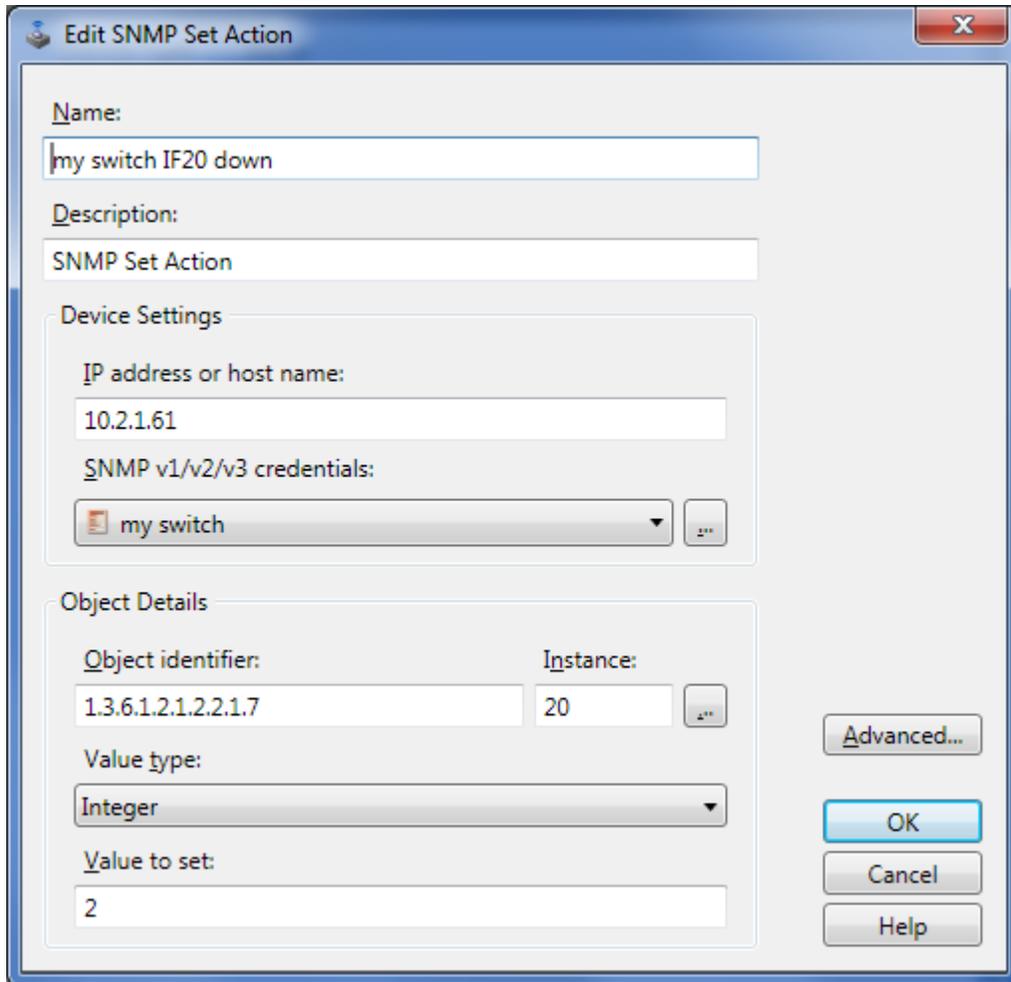
The screenshot shows a Windows-style dialog box titled "New SNMP Set Action". It contains several sections for configuring an SNMP action:

- Name:** A text field containing "my switch IF20 up".
- Description:** A text field containing "SNMP Set Action".
- Device Settings:** A section containing:
 - IP address or host name:** A text field containing "10.2.1.61".
 - SNMP v1/v2/v3 credentials:** A dropdown menu showing "my switch" and a "..." button to the right.
- Object Details:** A section containing:
 - Object identifier:** A text field containing "ifAdminStatus".
 - Instance:** A text field containing "20" and a "..." button to the right.
 - Value type:** A dropdown menu showing "Integer".
 - Value to set:** A text field containing "1".

On the right side of the dialog, there are four buttons: "Advanced...", "OK", "Cancel", and "Help".

Use the "copy" button to duplicate this action, and edit the copy as follows. Note that "Value to set" is now 2. Also note that the system automatically translated the object name to an OID.

We Bring Security To Light™



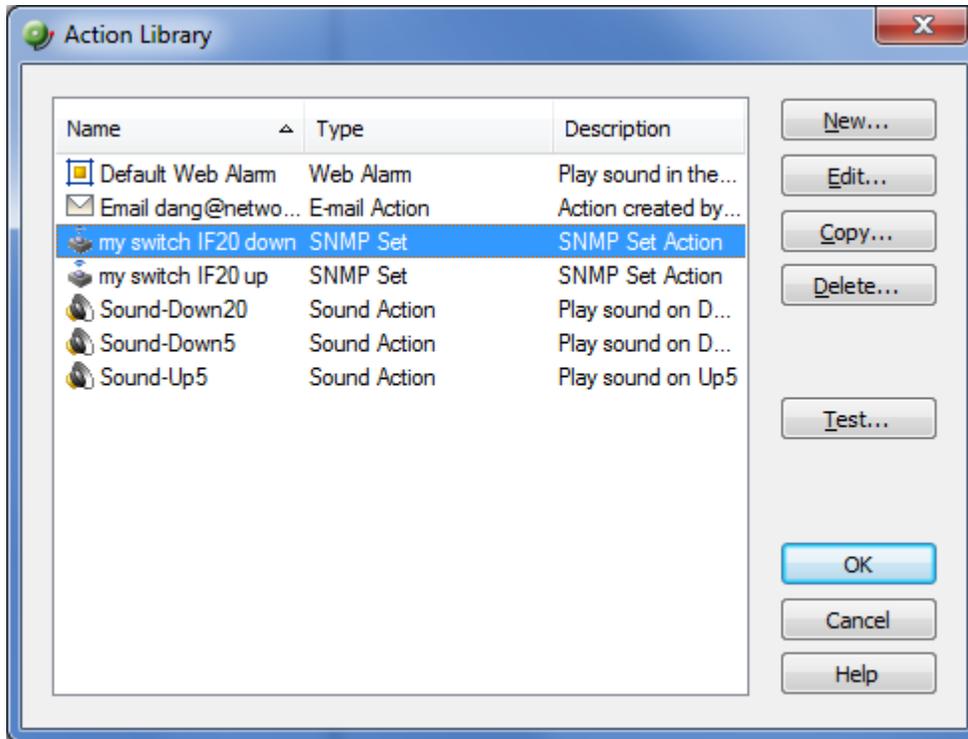
The screenshot shows a Windows-style dialog box titled "Edit SNMP Set Action". It contains several sections for configuring an SNMP set action:

- Name:** A text box containing "my switch IF20 down".
- Description:** A text box containing "SNMP Set Action".
- Device Settings:** A section containing:
 - IP address or host name:** A text box containing "10.2.1.61".
 - SNMP v1/v2/v3 credentials:** A dropdown menu showing "my switch" and a browse button "...".
- Object Details:** A section containing:
 - Object identifier:** A text box containing "1.3.6.1.2.1.2.2.1.7".
 - Instance:** A text box containing "20" and a browse button "...".
 - Value type:** A dropdown menu showing "Integer".
 - Value to set:** A text box containing "2".

On the right side of the dialog, there are four buttons: "Advanced...", "OK", "Cancel", and "Help".

The action library should now appear as follows...

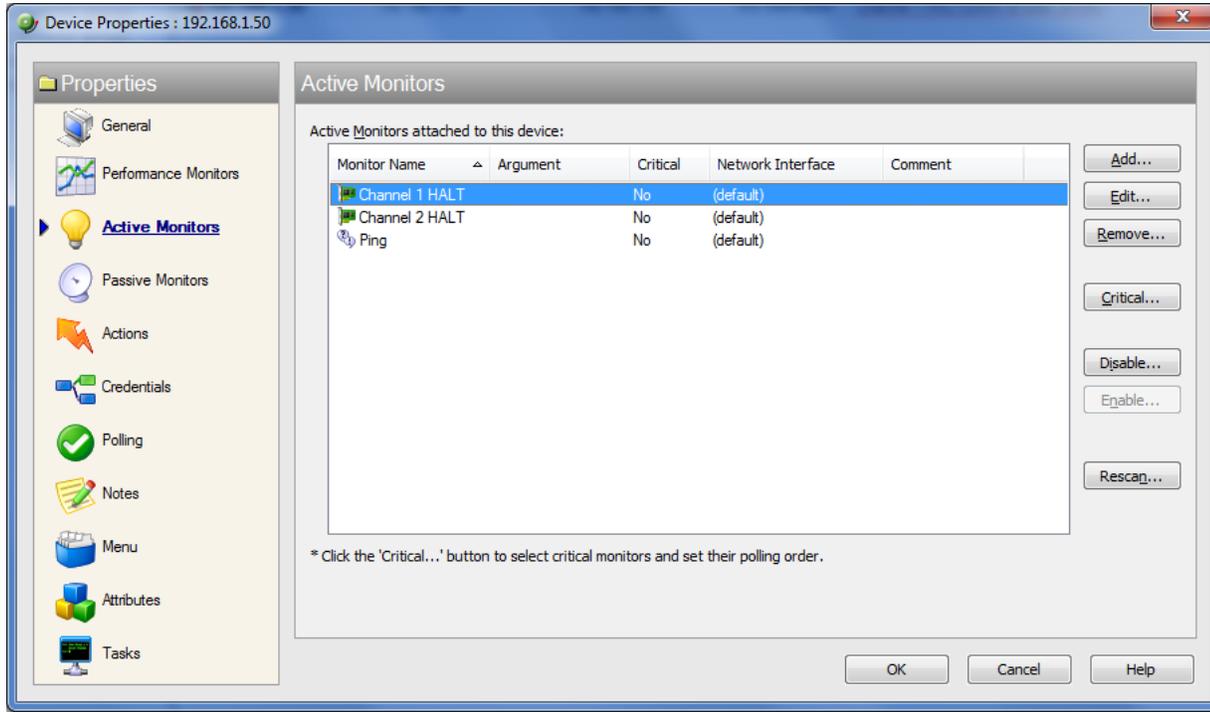
We Bring Security To Light™



4 Bind Interceptor Active Monitors to IF up/down actions

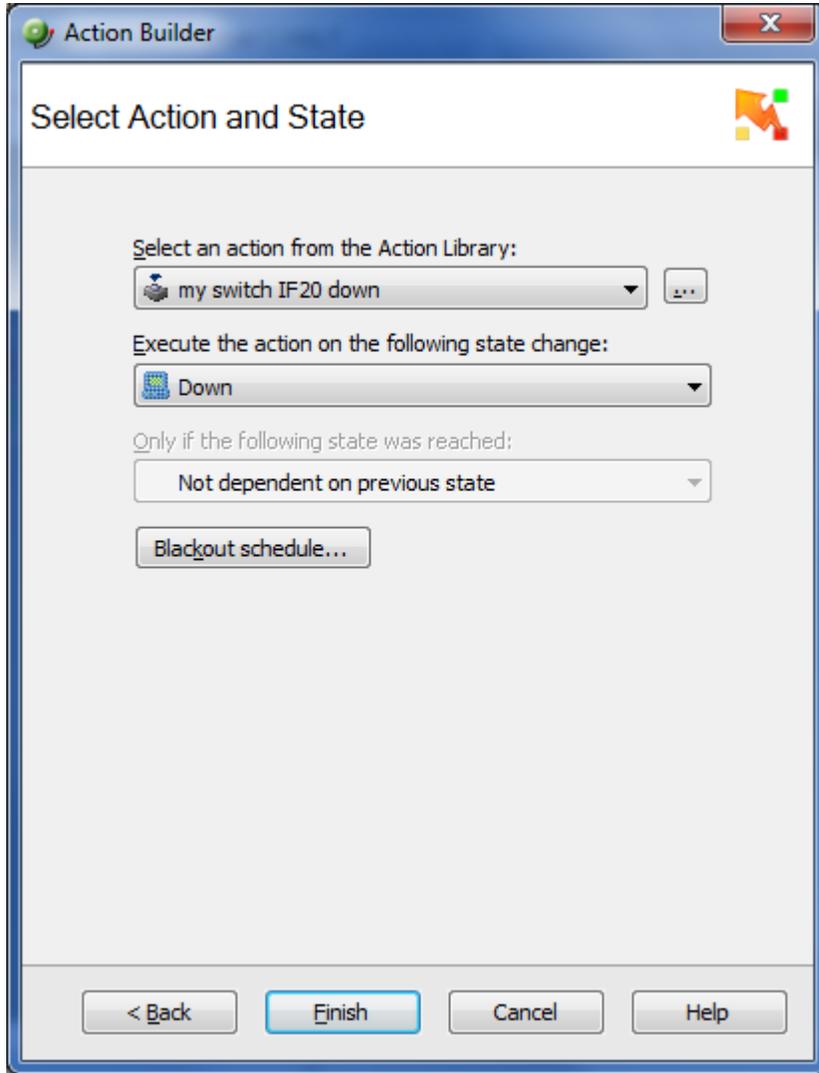
Now we will bind these actions to the up/down state of Interceptor channel 1. Double click on your Interceptor and examine the active monitors...

We Bring Security To Light™



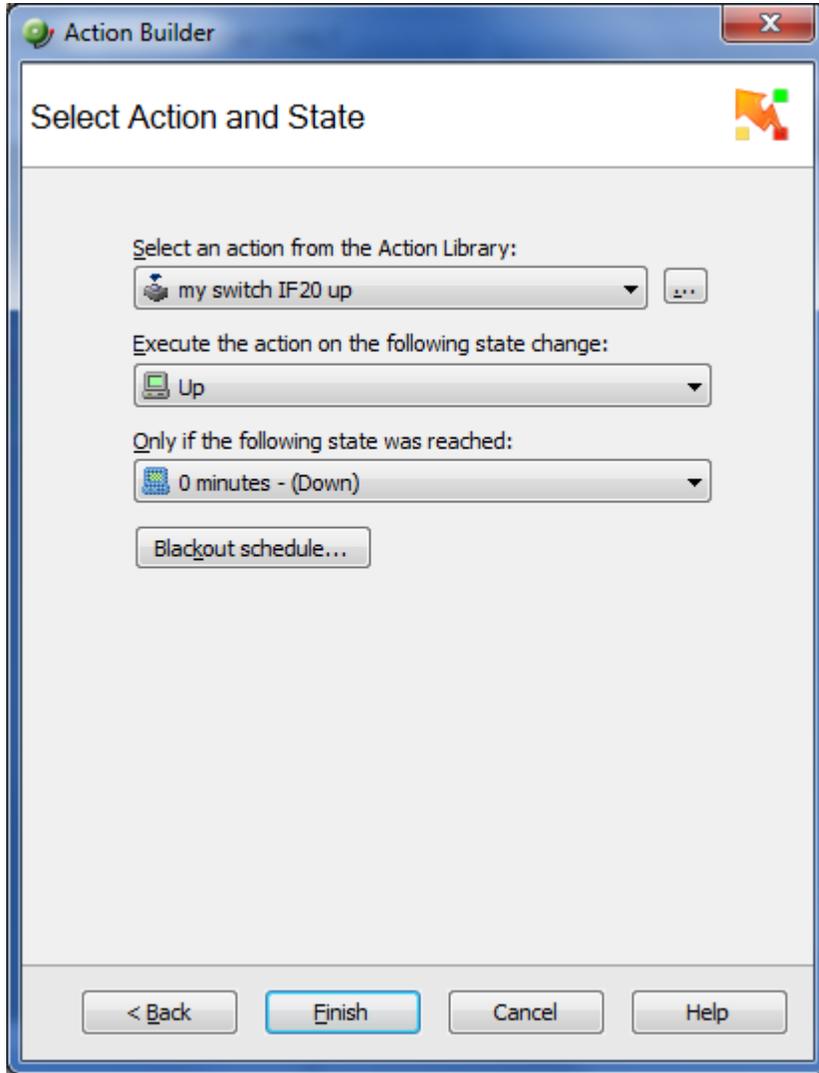
Edit "Channel 1 HALT", and then click Add. Pick "Chose an action from the action library", and then fill in the form as follows...

We Bring Security To Light™



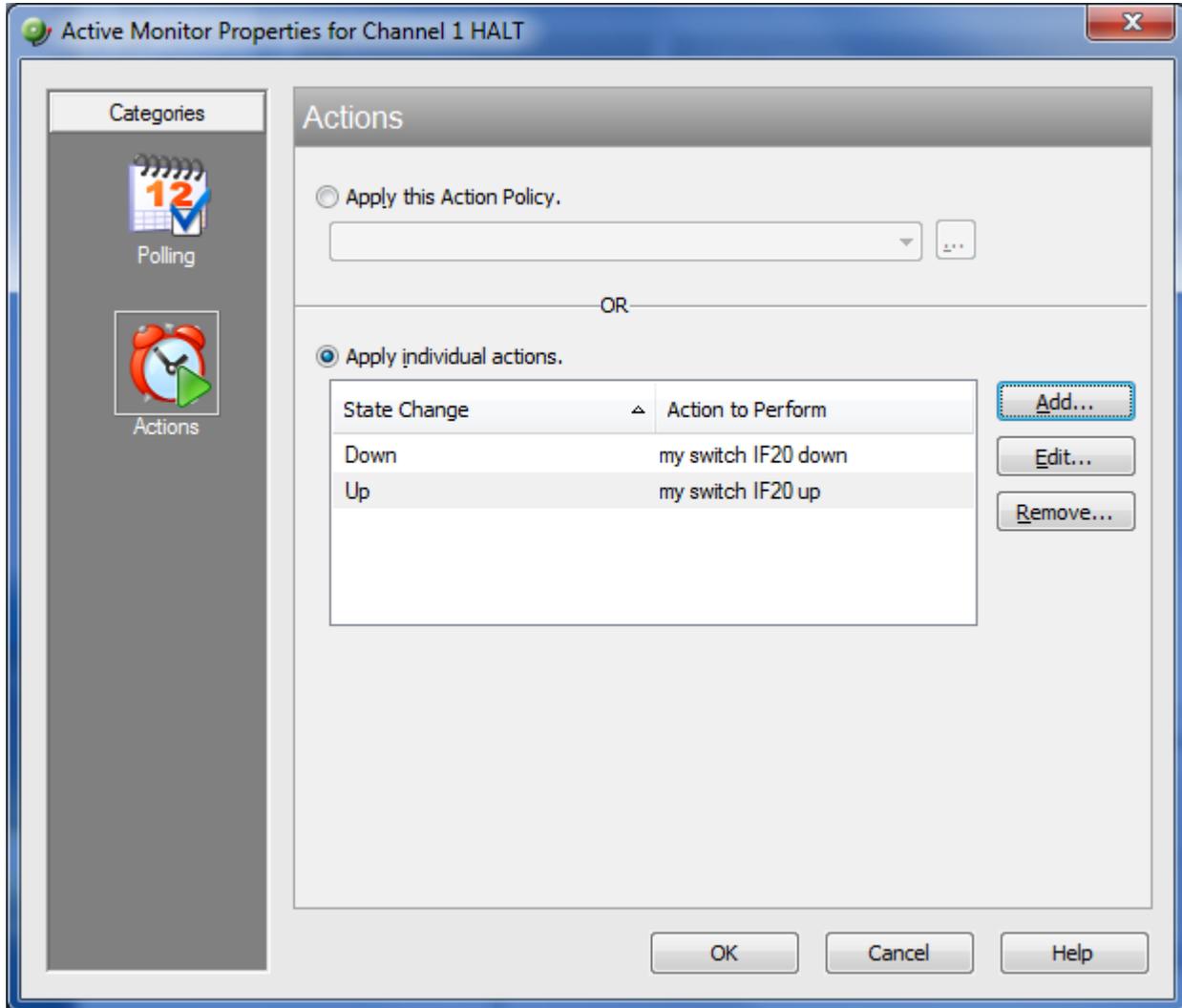
Repeat the process for the "Up" state. For "Up", the prior state must be specified...

We Bring Security To Light™



The completed action list should appear as follows...

We Bring Security To Light™



Click OK. The switch interface will now automatically go up and down in response to up/down transitions on the Interceptor channel....

We Bring Security To Light™

