

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 writeable variable that allows interfaces to be turned on and off. The OID for `ifAdminStatus` is ...

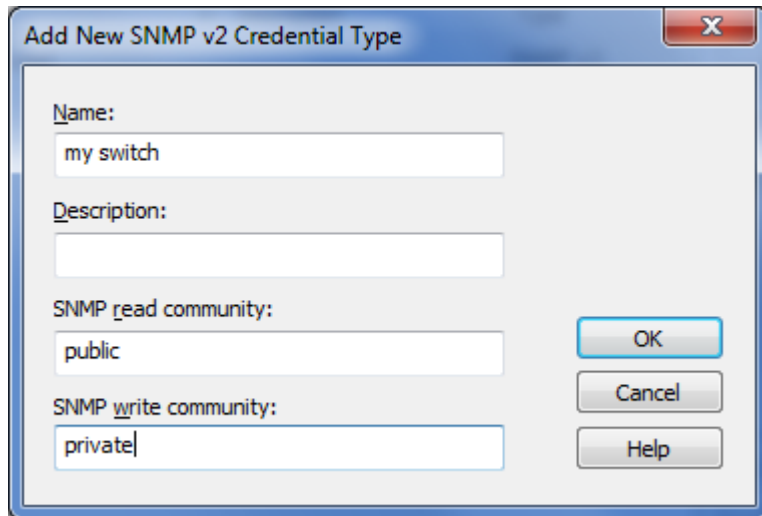
`1.3.6.1.2.1.2.2.1.7.x`

... 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.



Add New SNMP v2 Credential Type

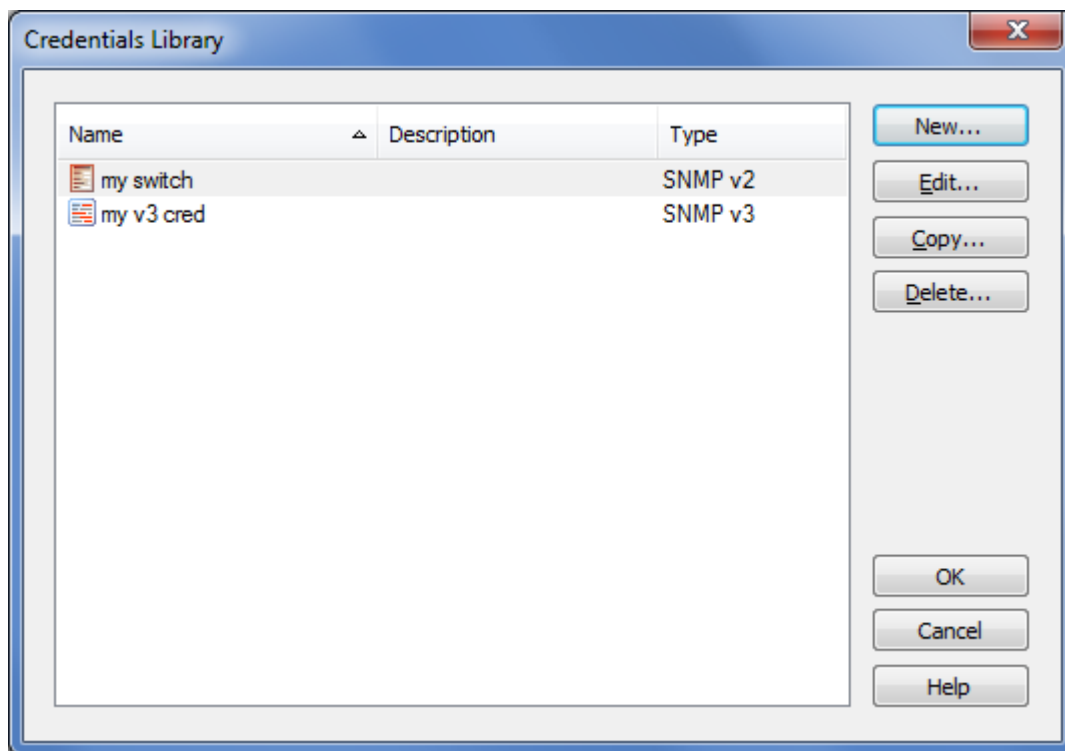
Name:
my switch

Description:

SNMP read community:
public

SNMP write community:
private

OK
Cancel
Help

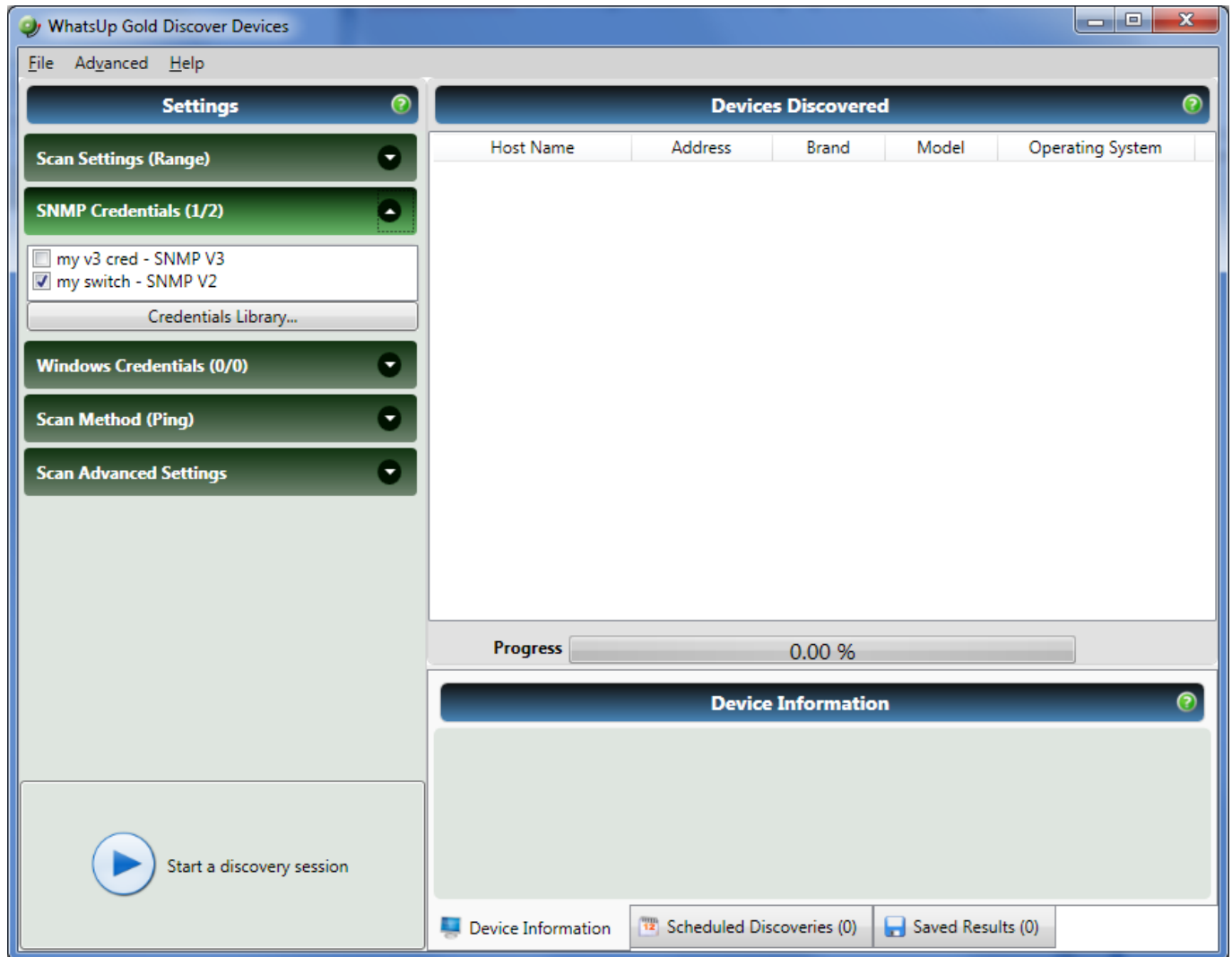


Credentials Library

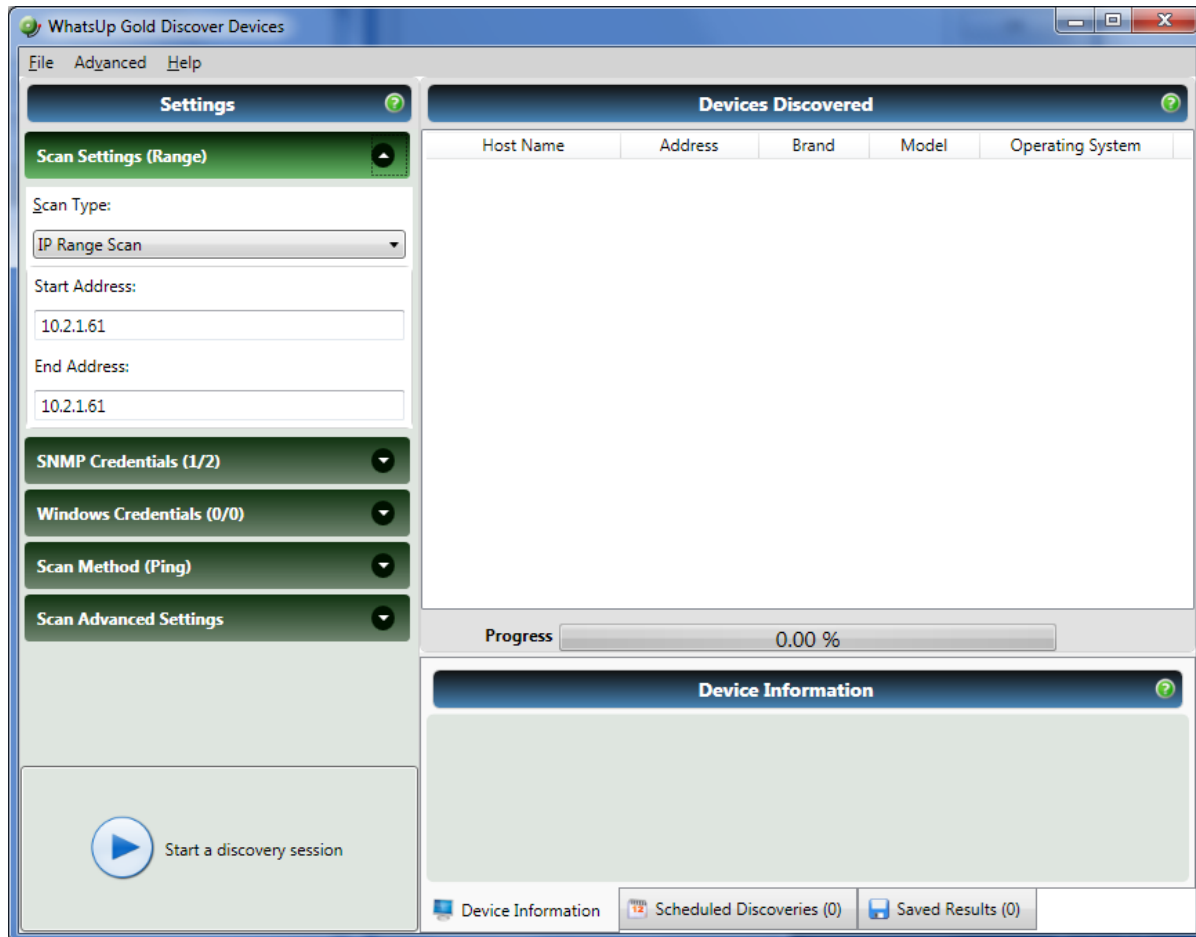
Name	Description	Type
my switch		SNMP v2
my v3 cred		SNMP v3

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

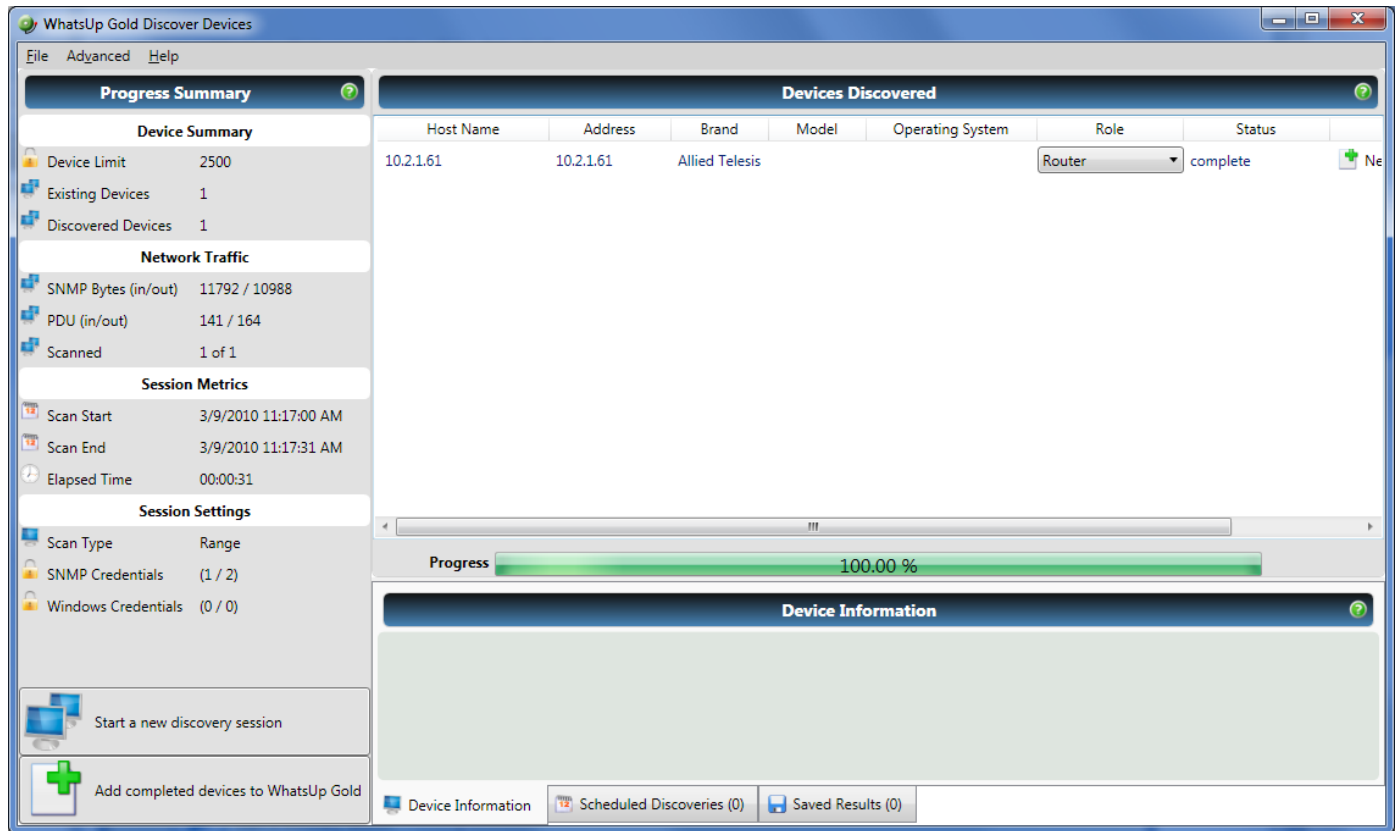
Next, get WUG to discover your device by clicking "Tools->Discover Devices...". Ensure your new SNMP credential is selected for the scan...



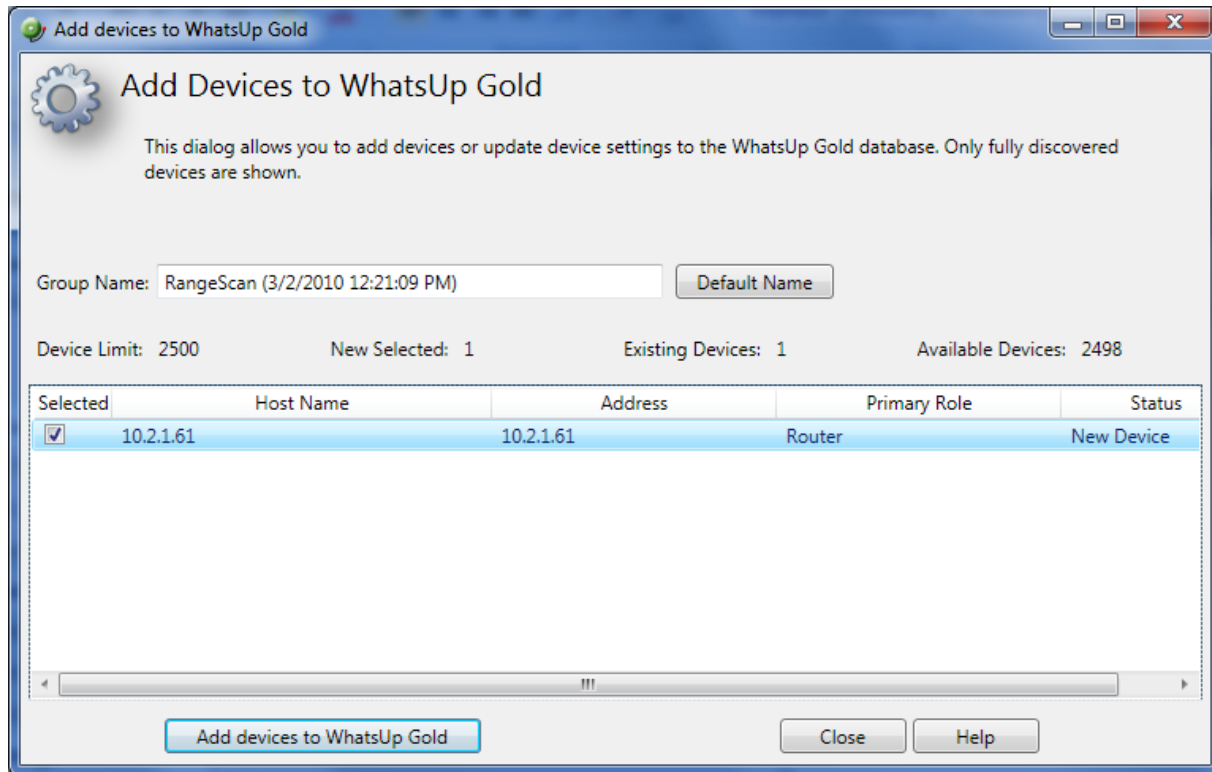
Adjust scan settings so that your switch will be detected...



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

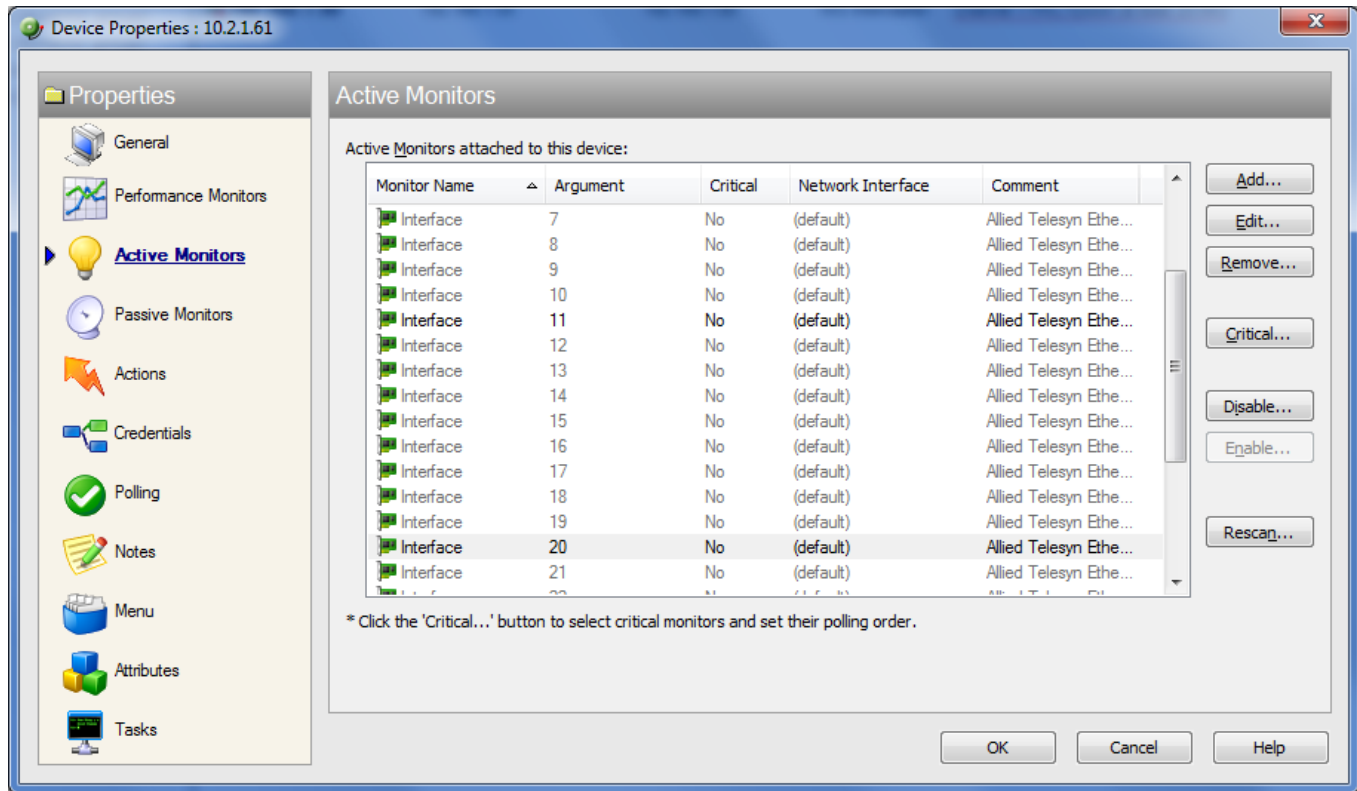


After this finishes, click "Add completed devices to WhatsUp Gold"...



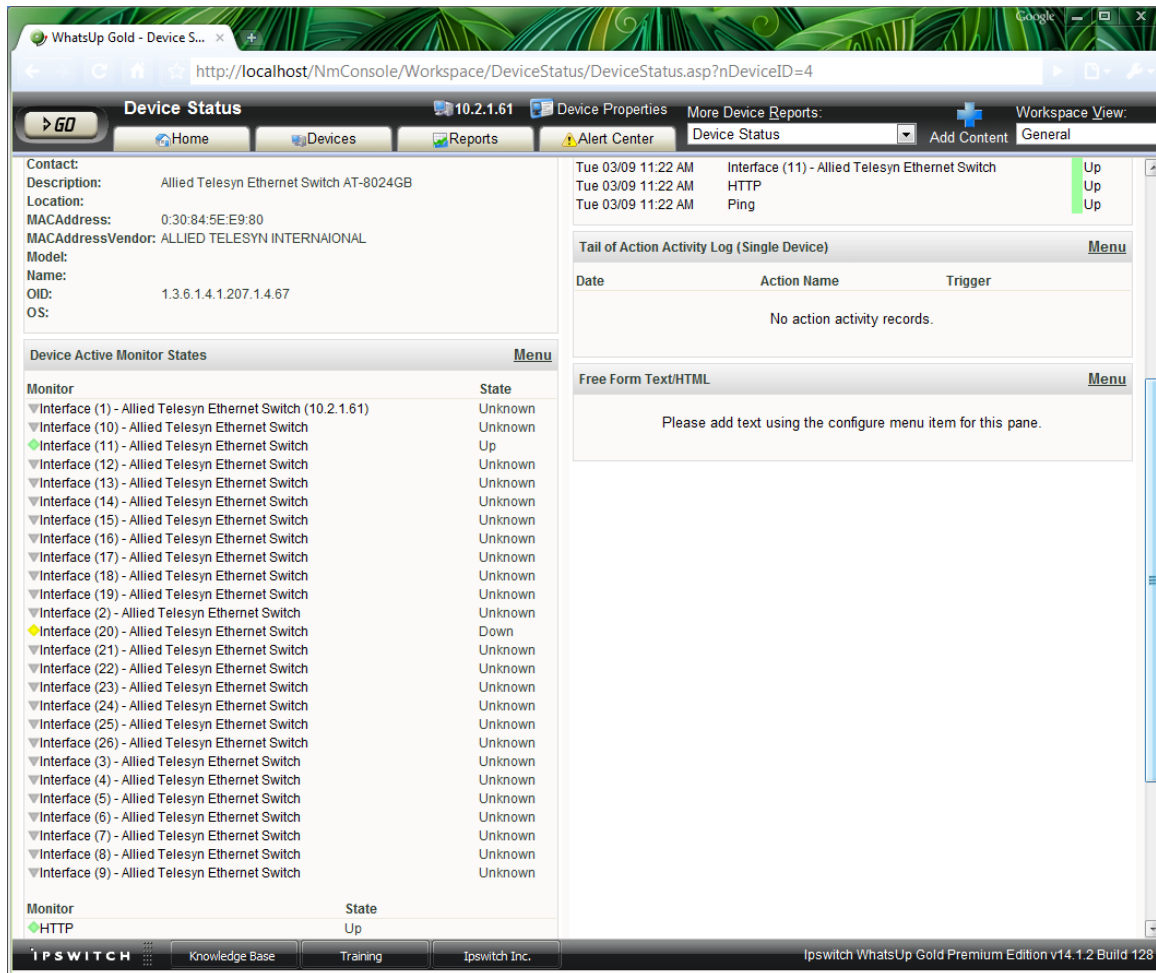
Select the switch, and click "Add devices to WhatsUp Gold". The switch will now have an Active Monitor for every interface in the switch. By default, monitors for interfaces that were down at detection time will be disabled. Double click on the device and click on "Active Monitors" to enable the monitors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



The screenshot shows the 'Device Status' page in the WhatsUp Gold interface. The browser address bar displays 'http://localhost/NmConsole/Workspace/DeviceStatus/DeviceStatus.asp?nDeviceID=4'. The page has a navigation bar with 'GO', 'Home', 'Devices', 'Reports', 'Alert Center', and 'More Device Reports: Device Status'. The main content area is divided into several sections:

- Contact Information:**
 - Description: Allied Telesyn Ethernet Switch AT-8024GB
 - Location:
 - MACAddress: 0:30:84:5E:E9:80
 - MACAddressVendor: ALLIED TELESYN INTERNAIONAL
 - Model:
 - Name:
 - OID: 1.3.6.1.4.1.207.1.4.67
 - OS:
- Device Active Monitor States:** A table listing various interfaces and their states.

Monitor	State
Interface (1) - Allied Telesyn Ethernet Switch (10.2.1.61)	Unknown
Interface (10) - Allied Telesyn Ethernet Switch	Unknown
Interface (11) - Allied Telesyn Ethernet Switch	Up
Interface (12) - Allied Telesyn Ethernet Switch	Unknown
Interface (13) - Allied Telesyn Ethernet Switch	Unknown
Interface (14) - Allied Telesyn Ethernet Switch	Unknown
Interface (15) - Allied Telesyn Ethernet Switch	Unknown
Interface (16) - Allied Telesyn Ethernet Switch	Unknown
Interface (17) - Allied Telesyn Ethernet Switch	Unknown
Interface (18) - Allied Telesyn Ethernet Switch	Unknown
Interface (19) - Allied Telesyn Ethernet Switch	Unknown
Interface (2) - Allied Telesyn Ethernet Switch	Unknown
Interface (20) - Allied Telesyn Ethernet Switch	Down
Interface (21) - Allied Telesyn Ethernet Switch	Unknown
Interface (22) - Allied Telesyn Ethernet Switch	Unknown
Interface (23) - Allied Telesyn Ethernet Switch	Unknown
Interface (24) - Allied Telesyn Ethernet Switch	Unknown
Interface (25) - Allied Telesyn Ethernet Switch	Unknown
Interface (26) - Allied Telesyn Ethernet Switch	Unknown
Interface (3) - Allied Telesyn Ethernet Switch	Unknown
Interface (4) - Allied Telesyn Ethernet Switch	Unknown
Interface (5) - Allied Telesyn Ethernet Switch	Unknown
Interface (6) - Allied Telesyn Ethernet Switch	Unknown
Interface (7) - Allied Telesyn Ethernet Switch	Unknown
Interface (8) - Allied Telesyn Ethernet Switch	Unknown
Interface (9) - Allied Telesyn Ethernet Switch	Unknown
- Interface Status Summary:**

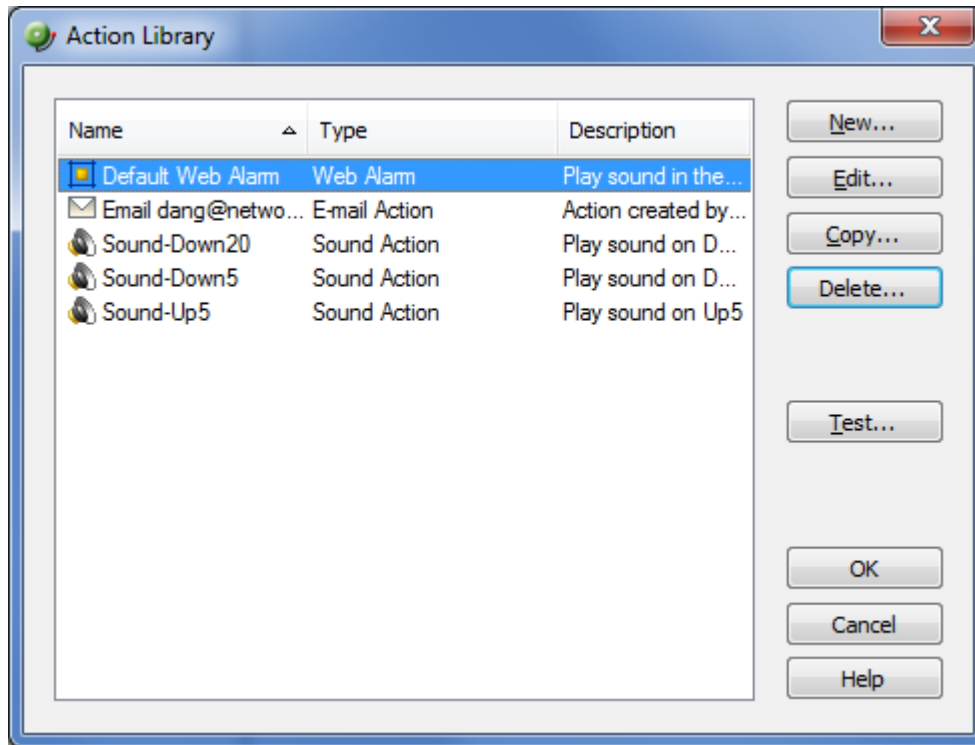
Date	Action Name	Trigger	State
Tue 03/09 11:22 AM	Interface (11) - Allied Telesyn Ethernet Switch		Up
Tue 03/09 11:22 AM	HTTP		Up
Tue 03/09 11:22 AM	Ping		Up
- Tail of Action Activity Log (Single Device):** A section with a 'Menu' button and a message: 'No action activity records.'
- Free Form Text/HTML:** A section with a 'Menu' button and a message: 'Please add text using the configure menu item for this pane.'

The bottom of the interface shows a status bar with 'IP SWITCH', 'Knowledge Base', 'Training', 'Ipswitch Inc.', and 'Ipswitch WhatsUp Gold Premium Edition v14.1.2 Build 128'.

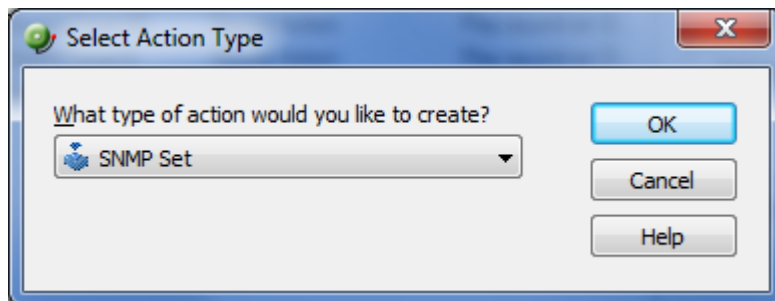
3 Add IF up/down actions

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..."

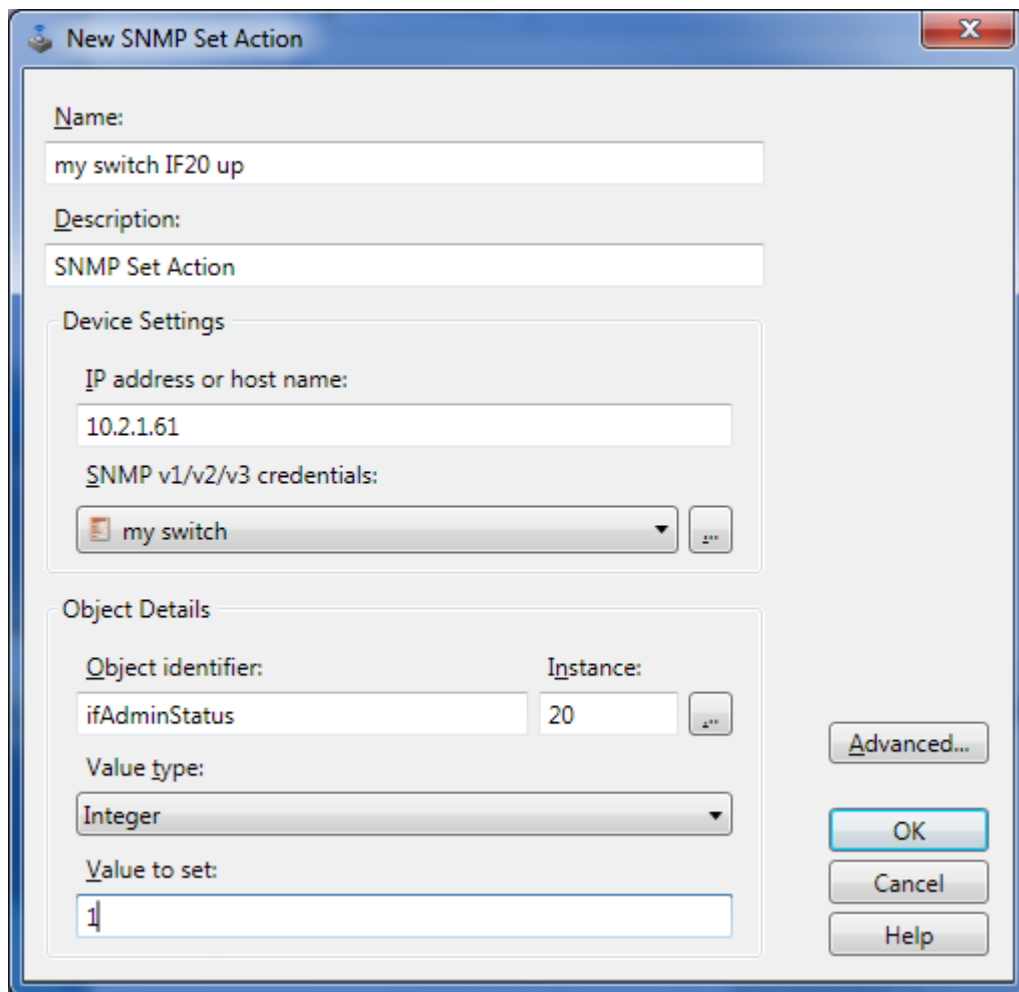
We Bring Security To Light™



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.



The image shows a Windows-style dialog box titled "New SNMP Set Action". It contains several input fields and buttons. The "Name" field is filled with "my switch IF20 up". The "Description" field is filled with "SNMP Set Action". Under the "Device Settings" section, the "IP address or host name" field is filled with "10.2.1.61", and the "SNMP v1/v2/v3 credentials" dropdown menu is set to "my switch". Under the "Object Details" section, the "Object identifier" field is filled with "ifAdminStatus", the "Instance" field is filled with "20", the "Value type" dropdown menu is set to "Integer", and the "Value to set" field is filled with "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.

Edit SNMP Set Action

Name: my switch IF20 down

Description: SNMP Set Action

Device Settings

IP address or host name: 10.2.1.61

SNMP v1/v2/v3 credentials: my switch

Object Details

Object identifier: 1.3.6.1.2.1.2.2.1.7 Instance: 20

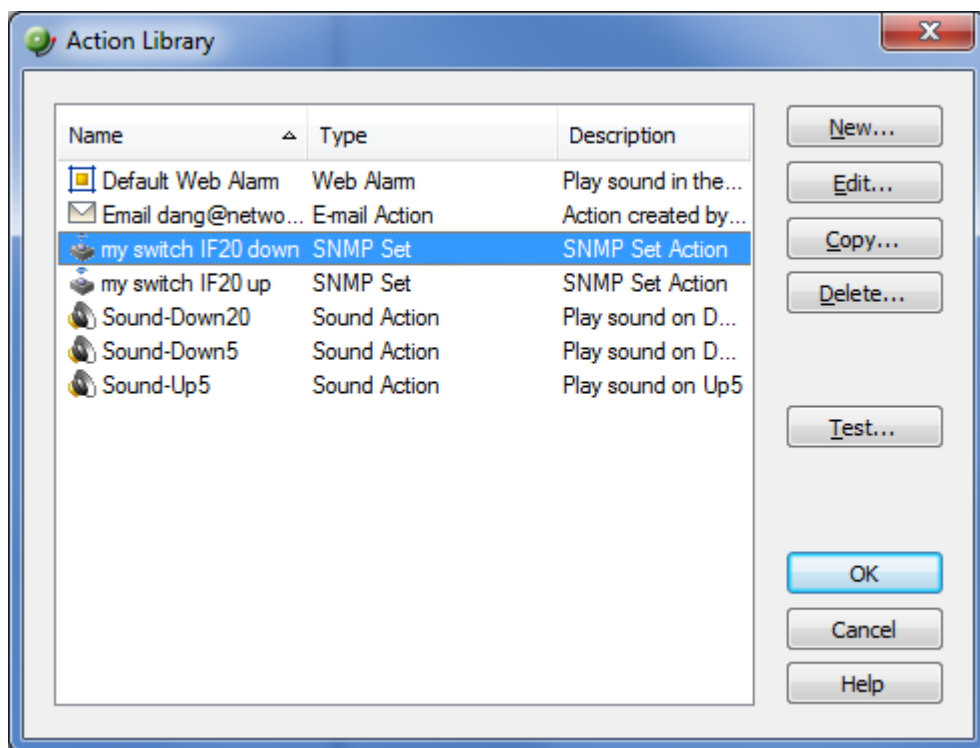
Value type: Integer

Value to set: 2

Advanced... OK Cancel Help

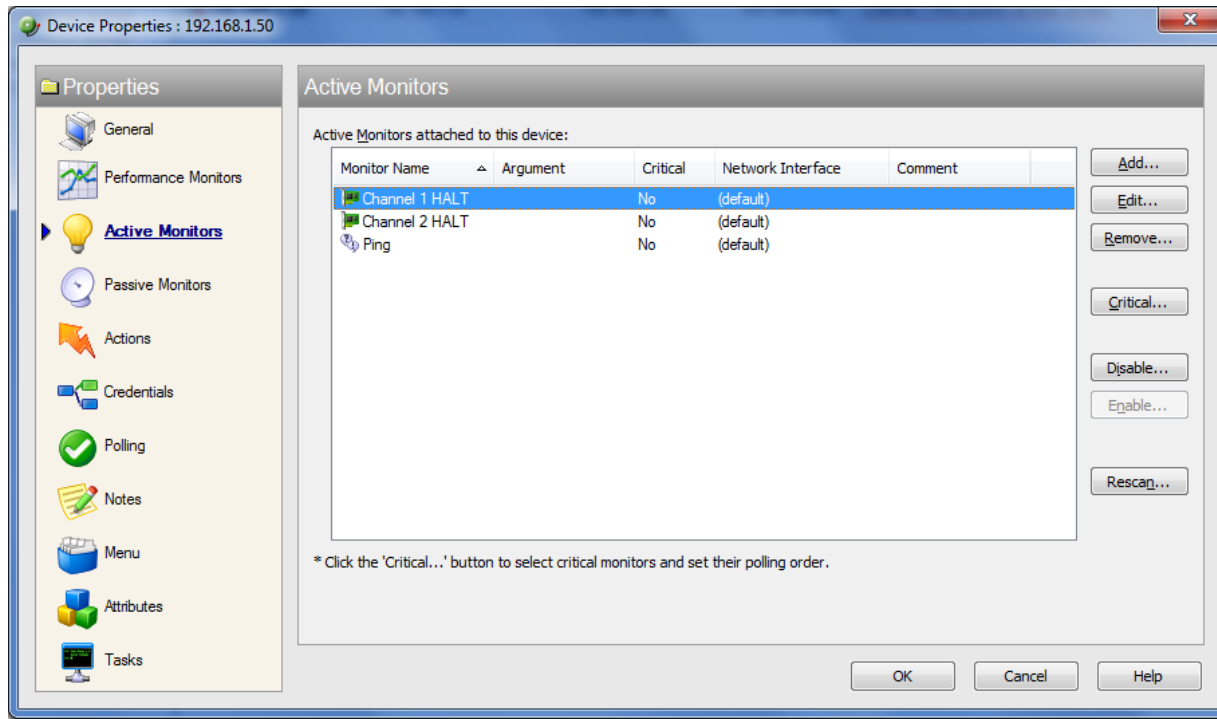
The action library should now appear as follows...

We Bring Security To Light™

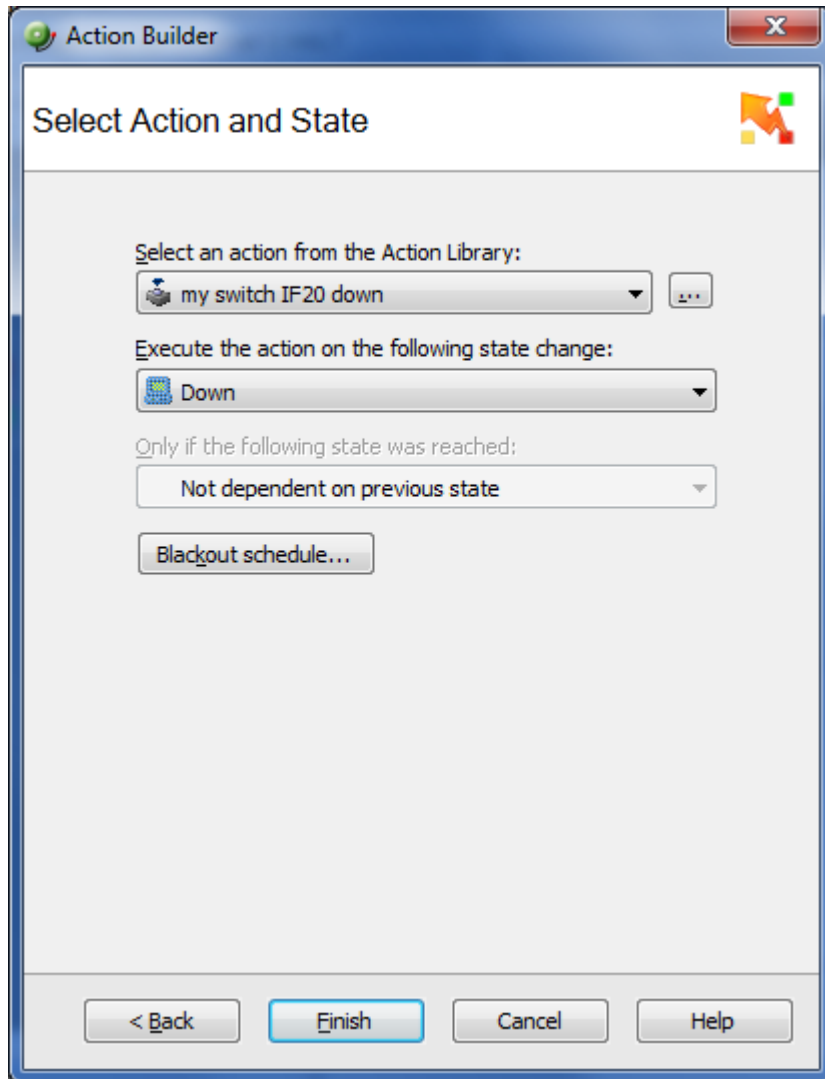


4 Bind Interceptor Active Monitors to IF up/down actions

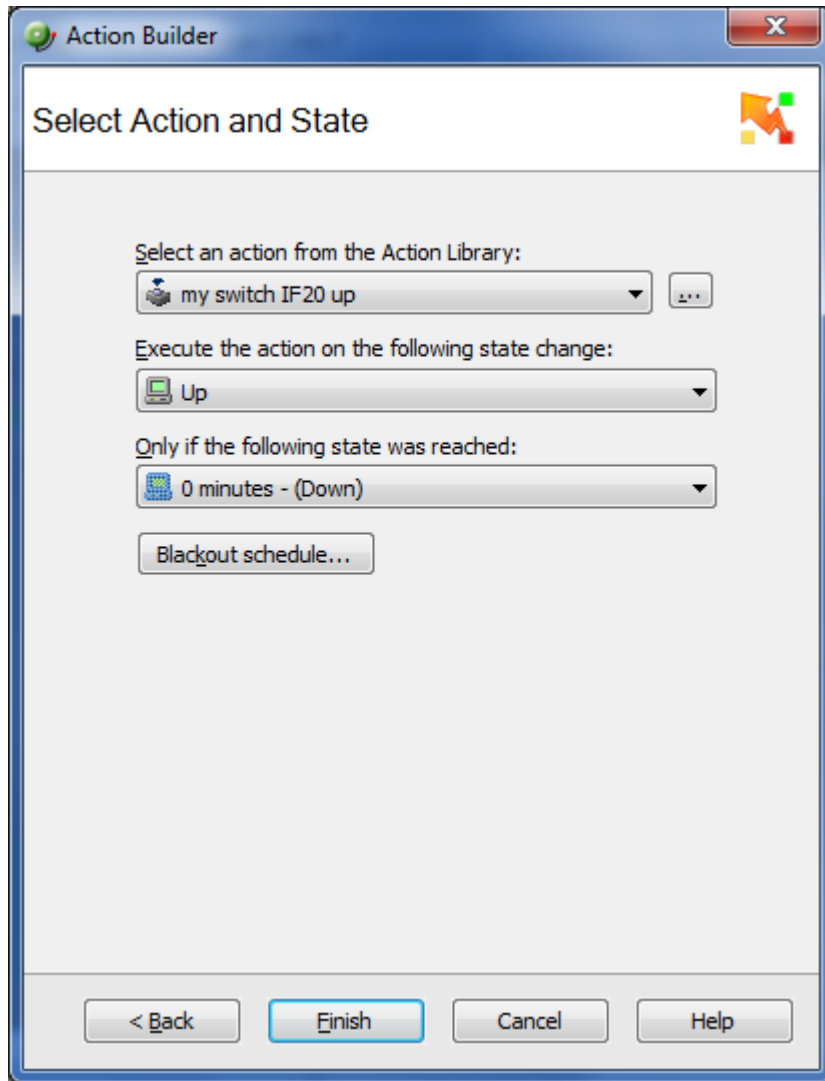
Now we will bind these actions to the up/down state of Interceptor channel 1. Double click on your Interceptor and examine the active monitors...



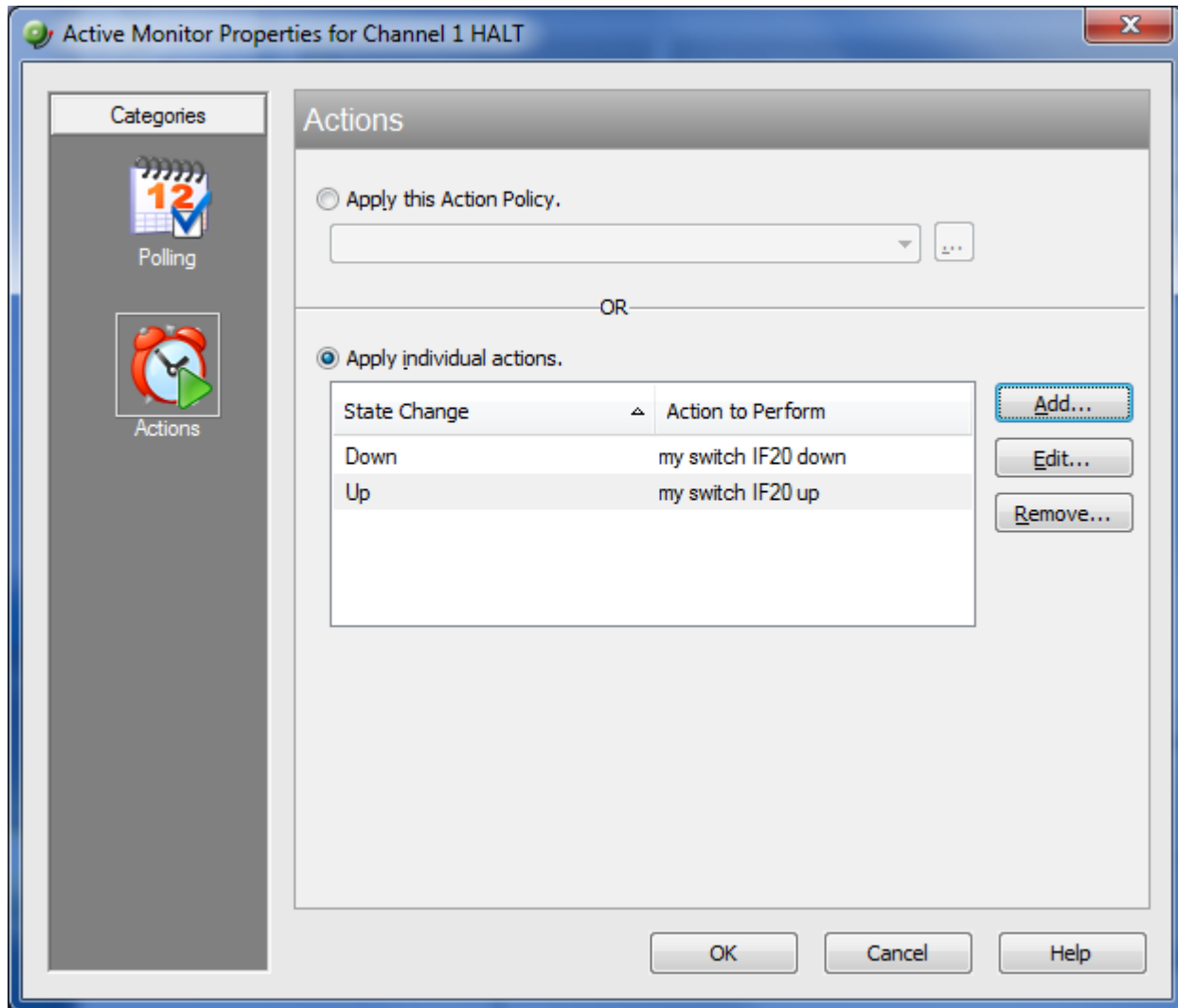
Edit "Channel 1 HALT", and then click Add. Pick "Chose an action from the action library", and then fill in the form as follows...



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



The completed action list should appear as follows...



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™

