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 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".

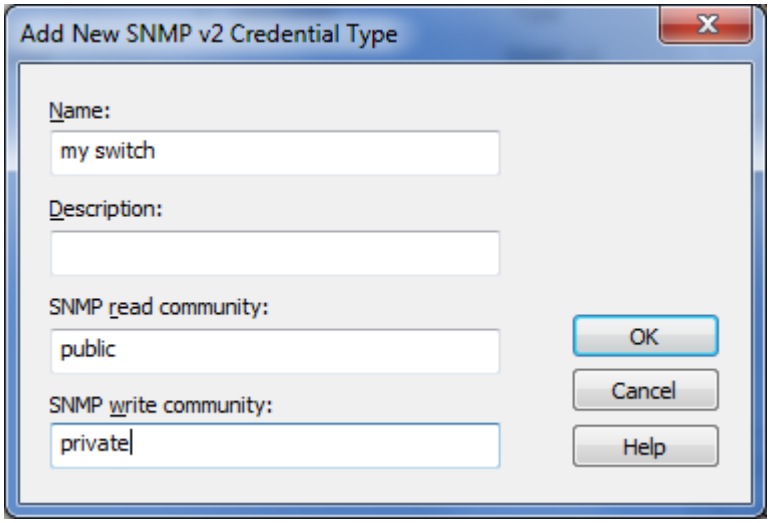
2 Add your switch

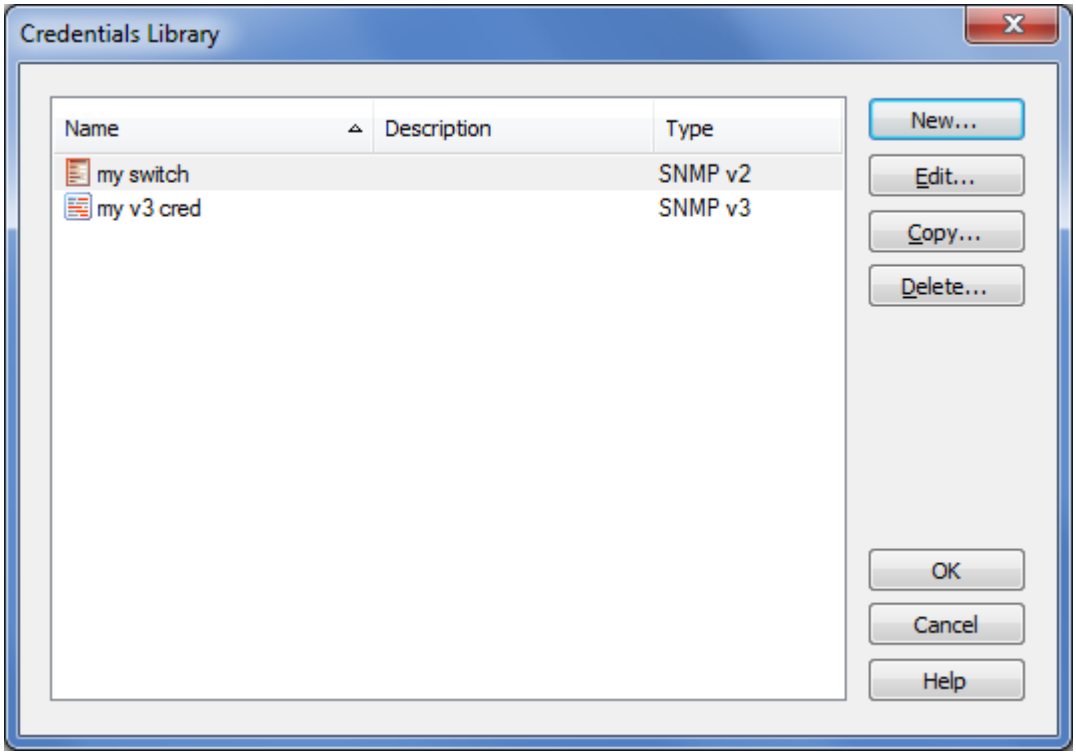
WUG must know about your switch to be able to control it. First, add an SNMP credential by clicking "Configure->Credentials...", then "New". The example below shows the creation of an SNMP v2 credential. SNMP v3 is preferred if your switch supports it.

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™



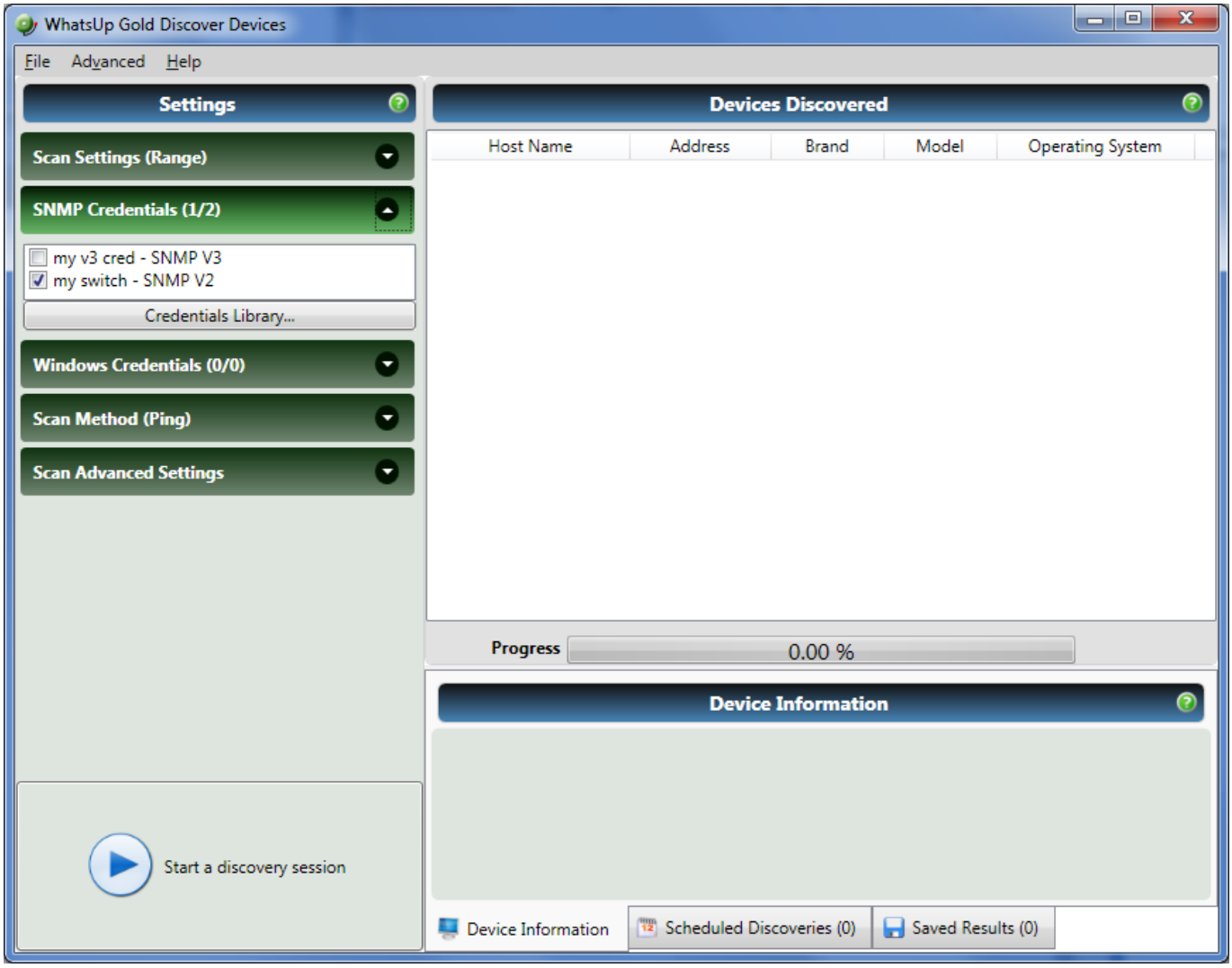


Next, get WUG to discover your device by clicking "Tools->Discover Devices...". Ensure your new SNMP credential is selected for the scan...

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™

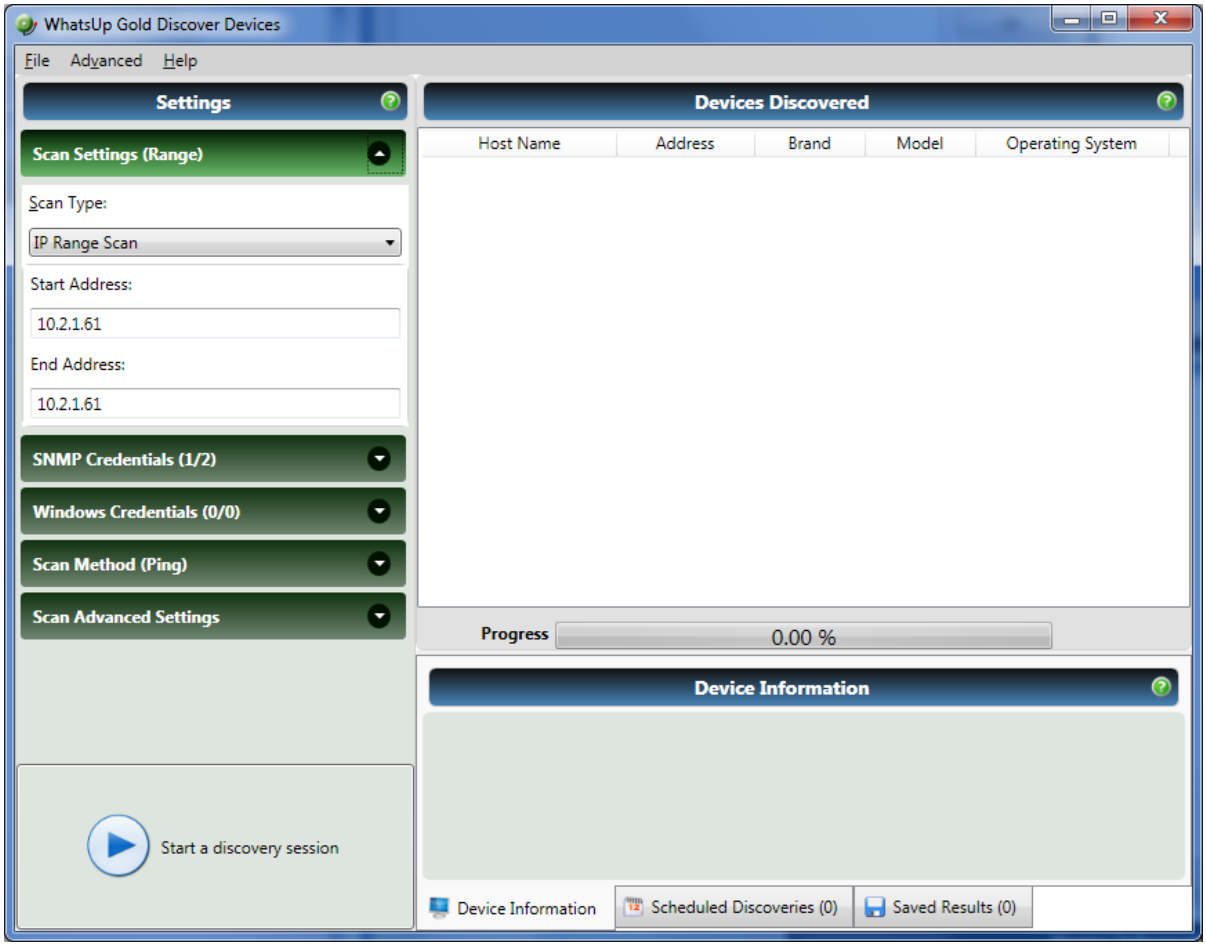


Adjust scan settings so that your switch will be detected...

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™

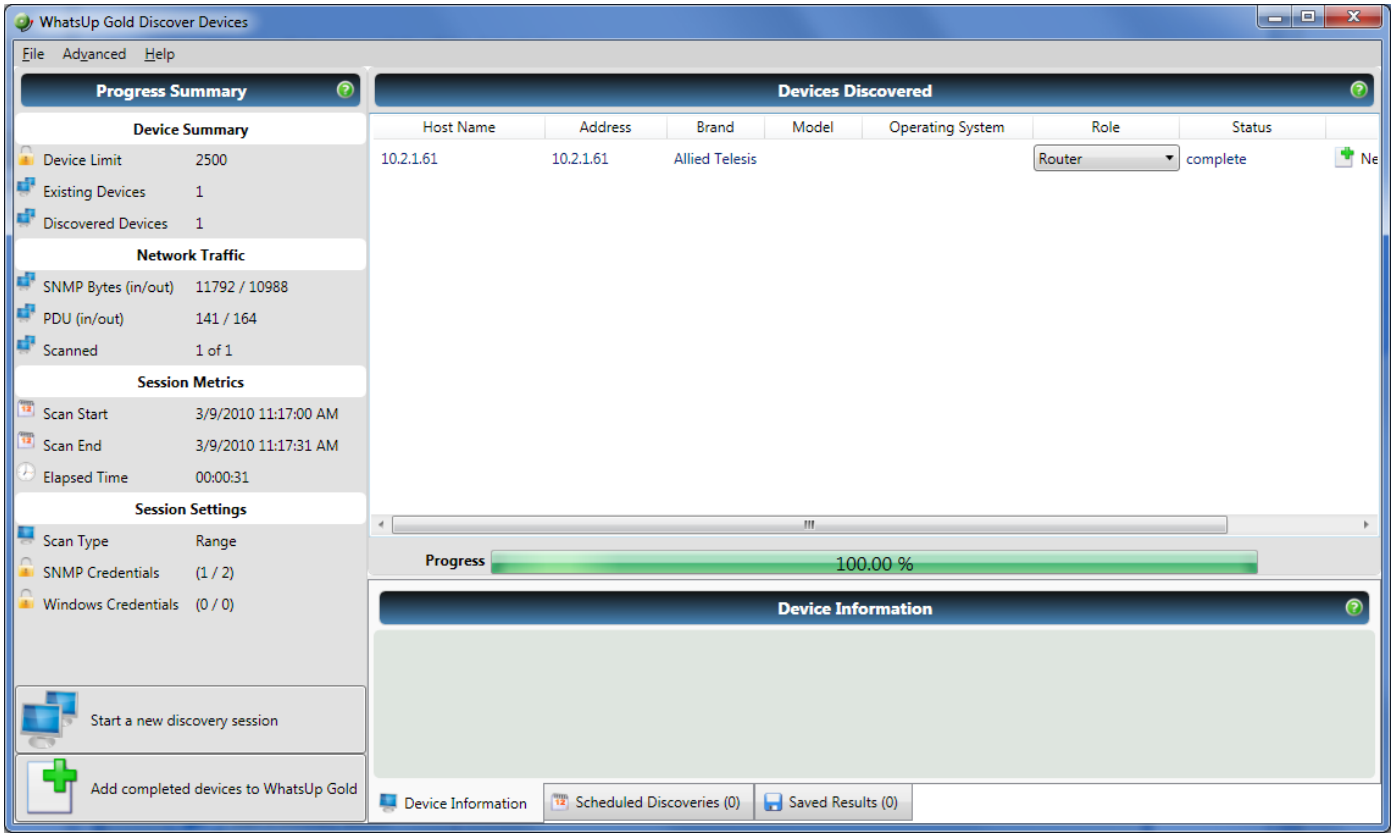


Click "Start a discovery session" to discover your switch...

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™

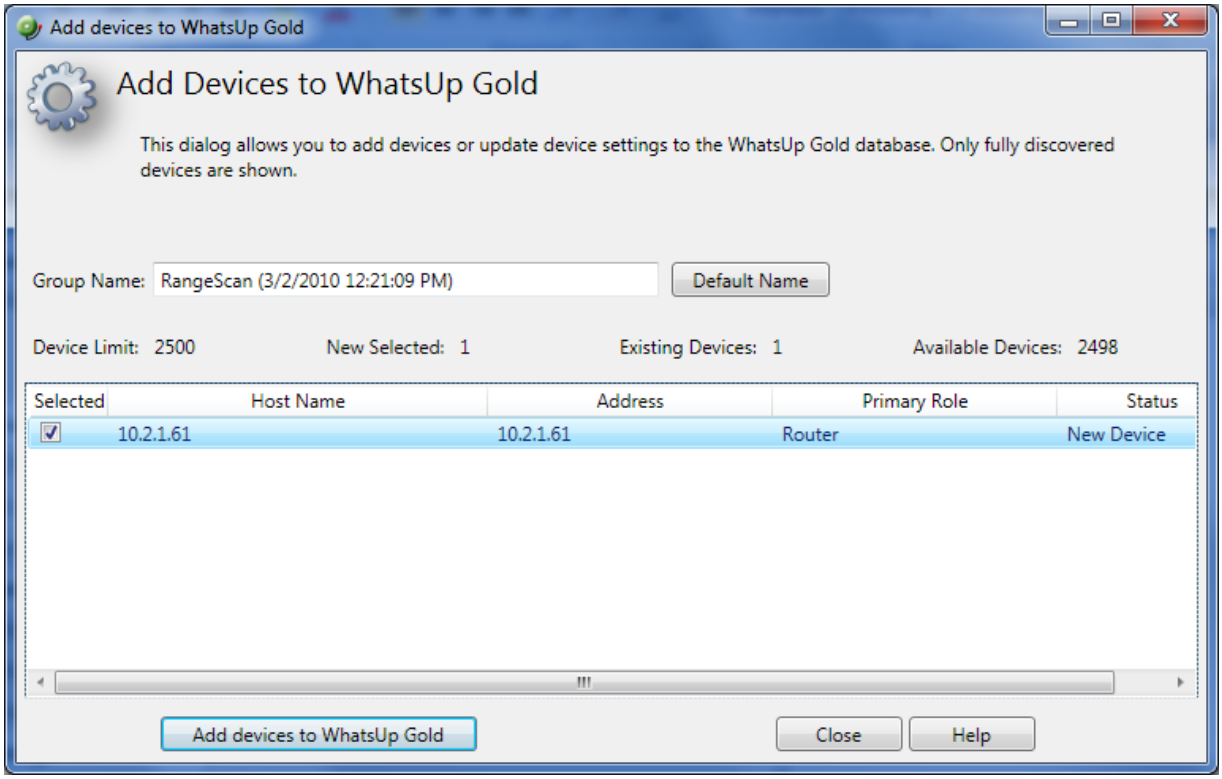


After this finishes, click "Add completed devices to WhatsUp Gold"...

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™

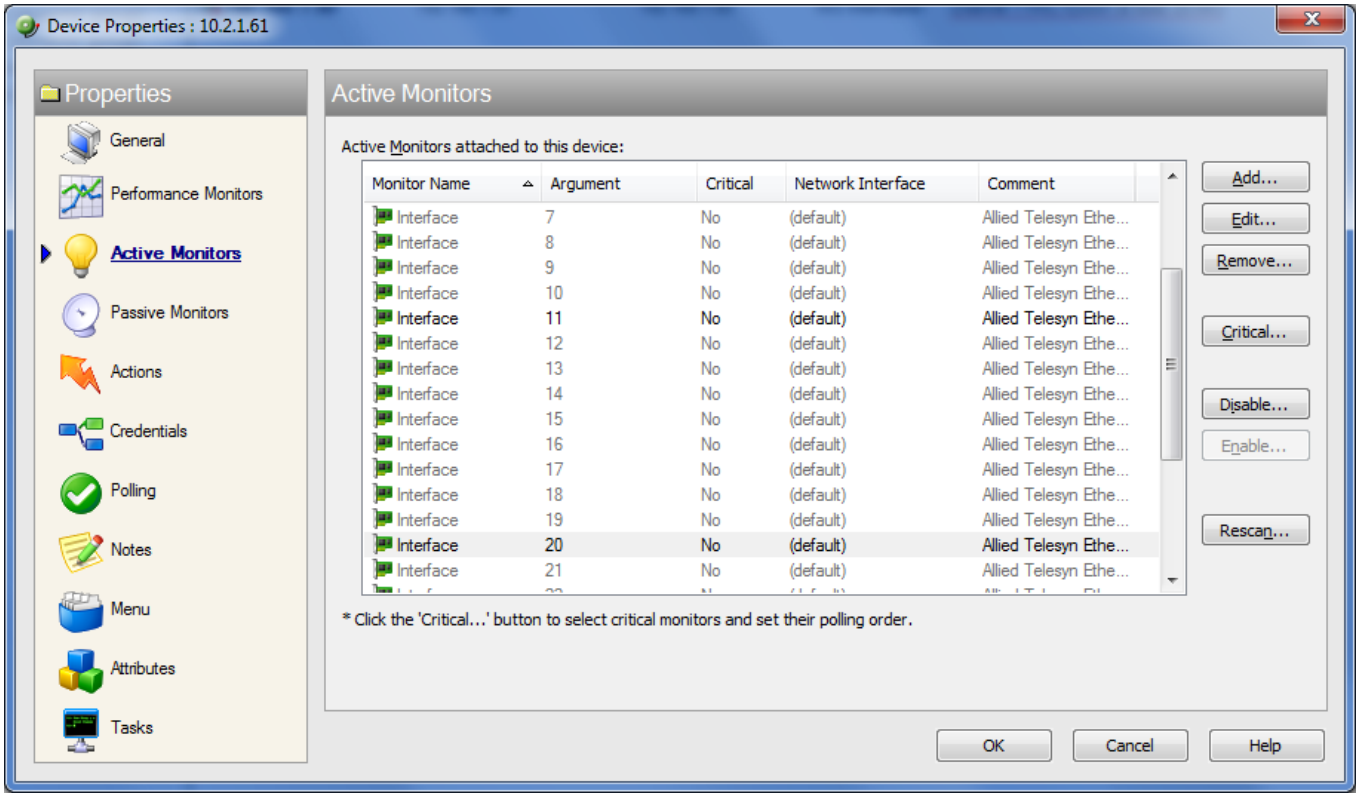


Select the switch, and click "Add devices to WhatsUp Gold". The switch will now have an Active Monitor for every interface in the switch. By default, monitors for interfaces that were down at detection time will be disabled. Double click on the device and click on "Active Monitors" to enable the monitors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

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™

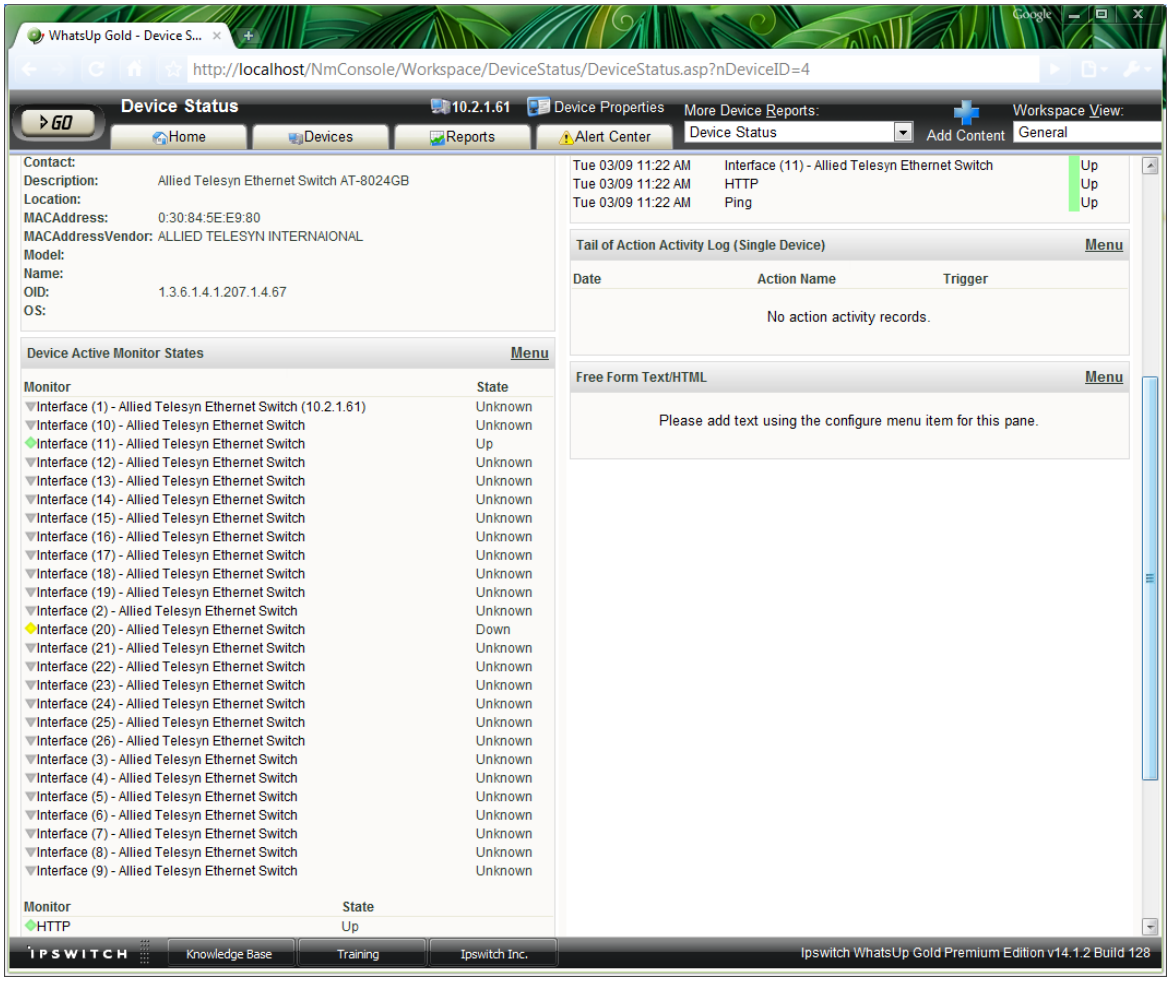


View the switch through the WUG web interface to confirm that it is being monitored properly...

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™

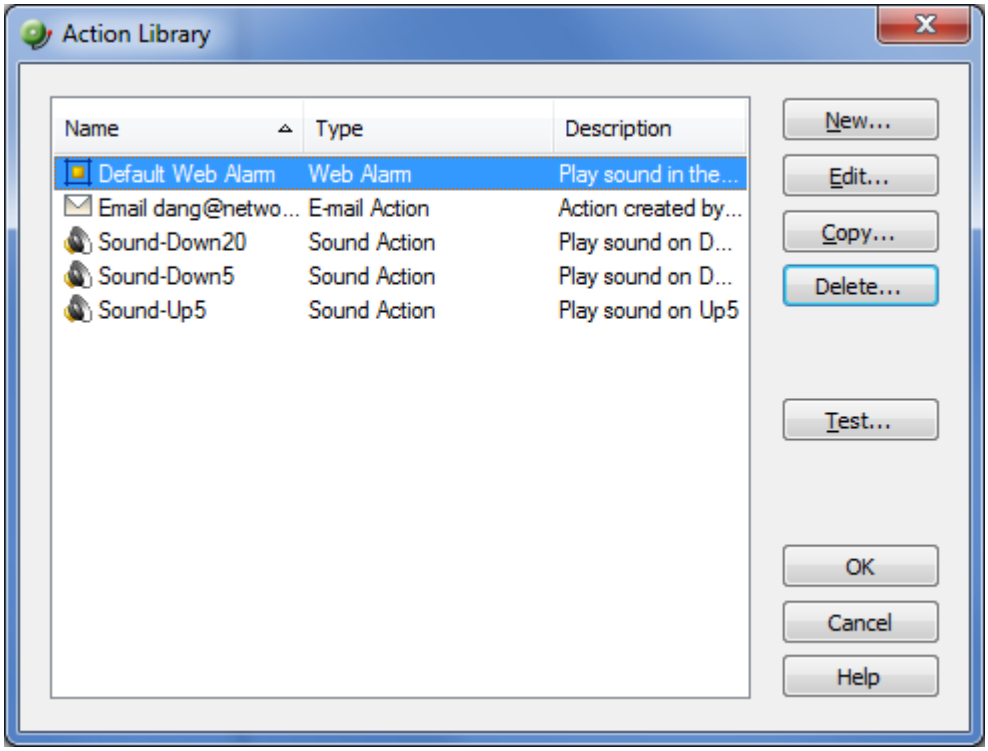


3 *Add IF up/down actions*

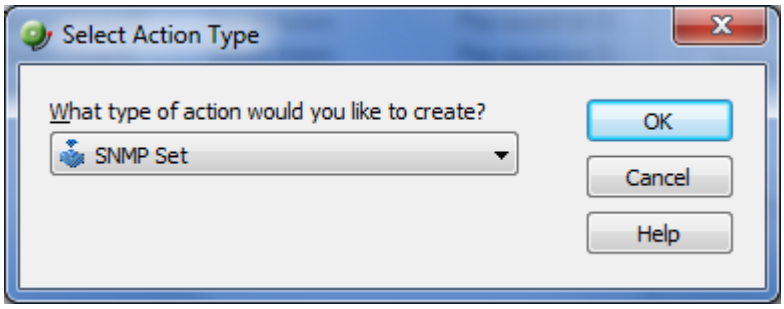
Now we will add Actions to bring interfaces up and down. For this example, we will add actions to control interface 20. Click "Configure->Action Library..."

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

info@networkintegritysystems.com
www.networkintegritysystems.com



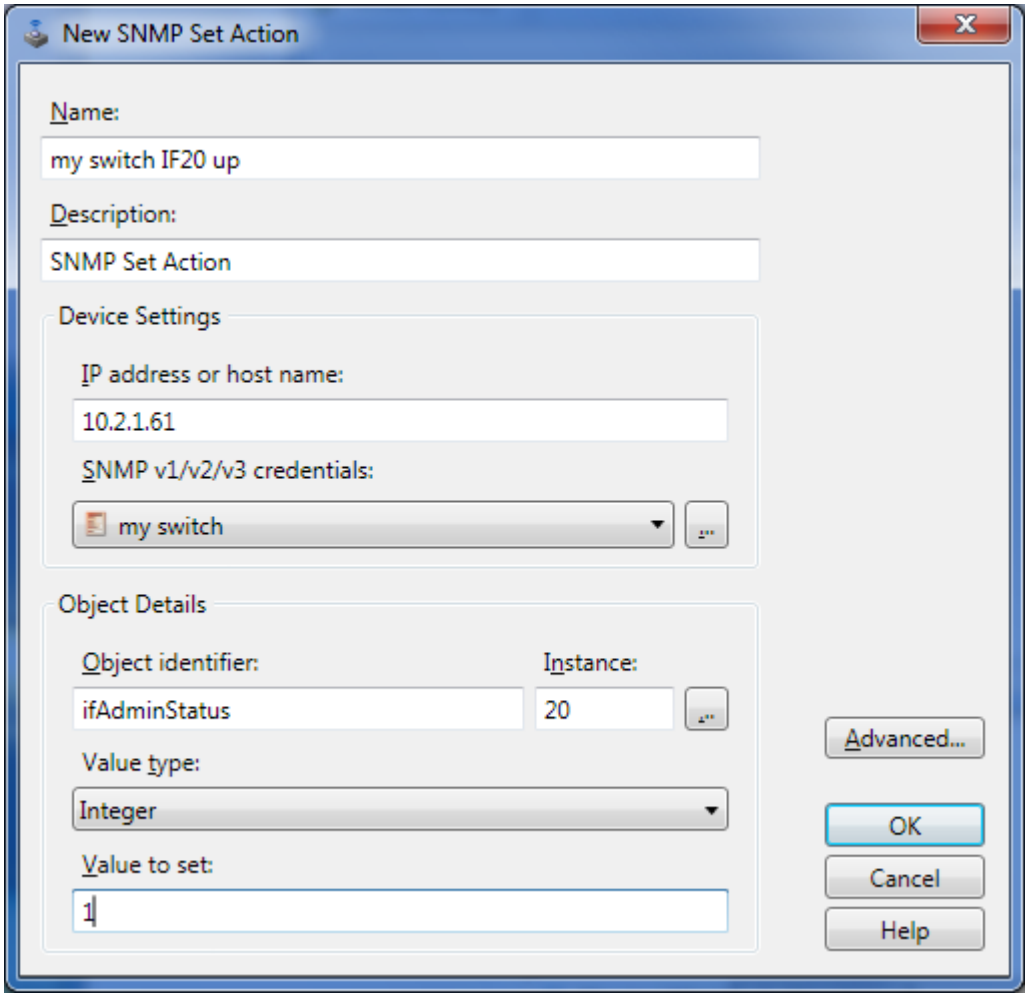
Click "New" and select SNMP Set...



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

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

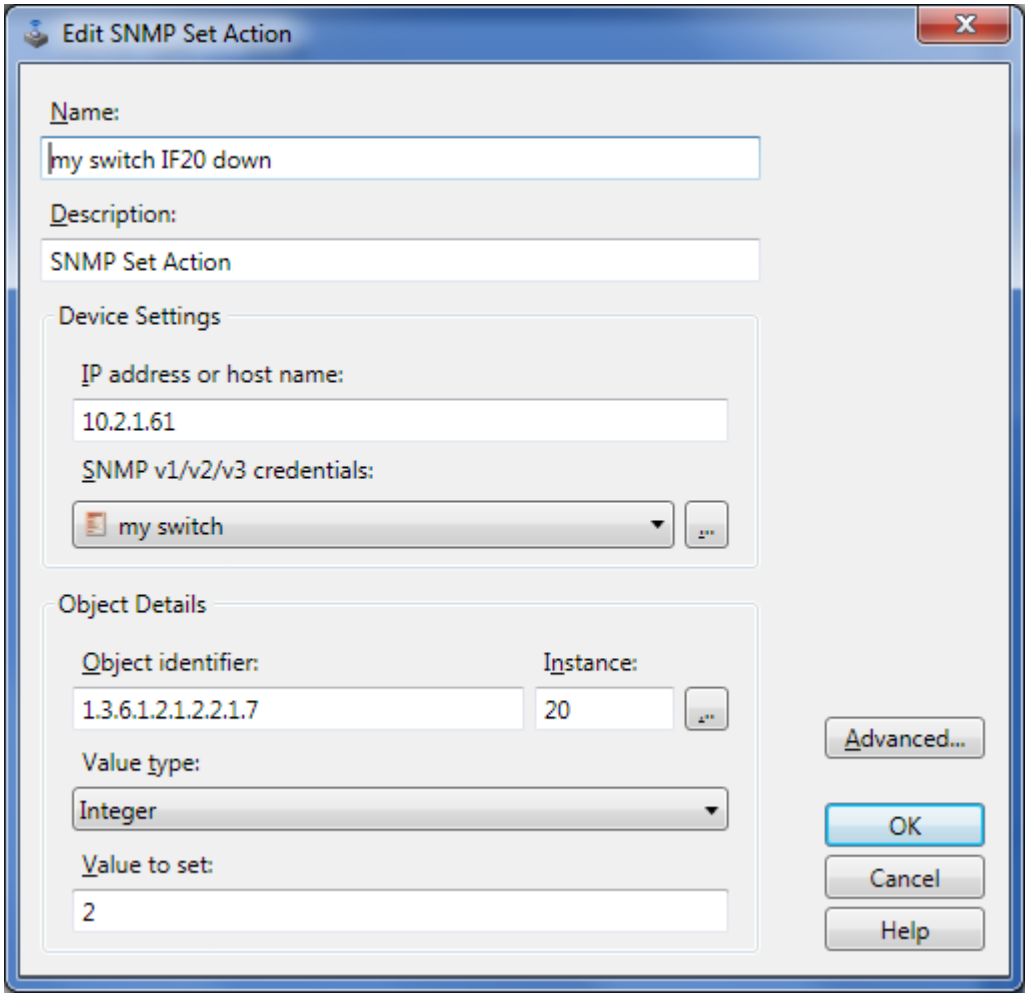
info@networkintegritysystems.com
www.networkintegritysystems.com



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.

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

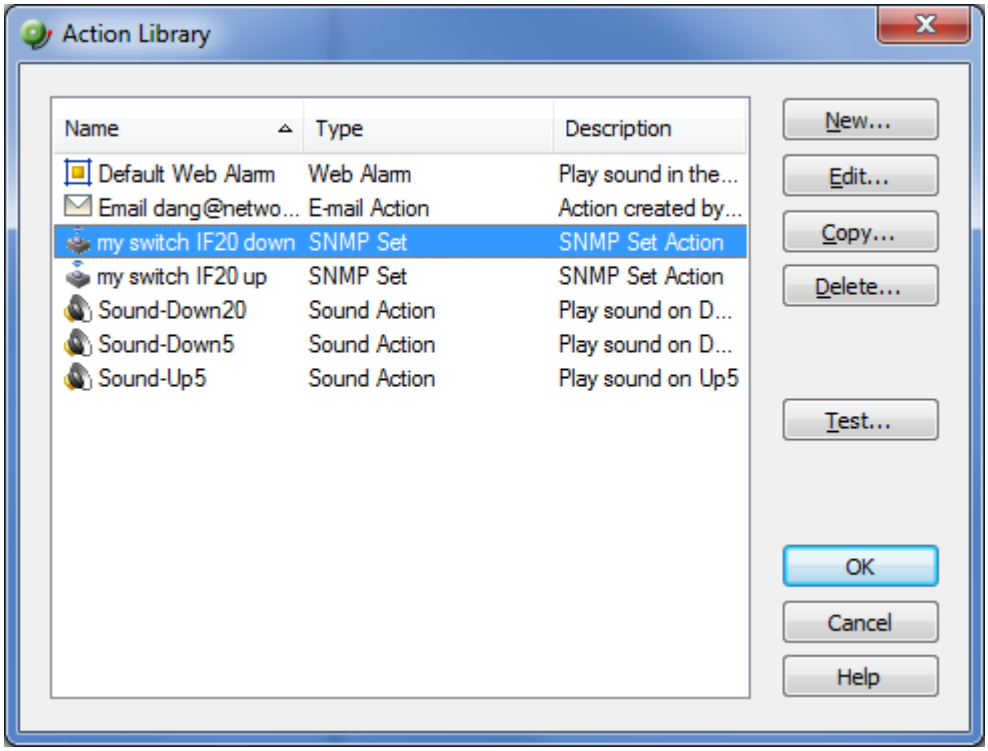
info@networkintegritysystems.com
www.networkintegritysystems.com



The action library should now appear as follows...

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

info@networkintegritysystems.com
www.networkintegritysystems.com

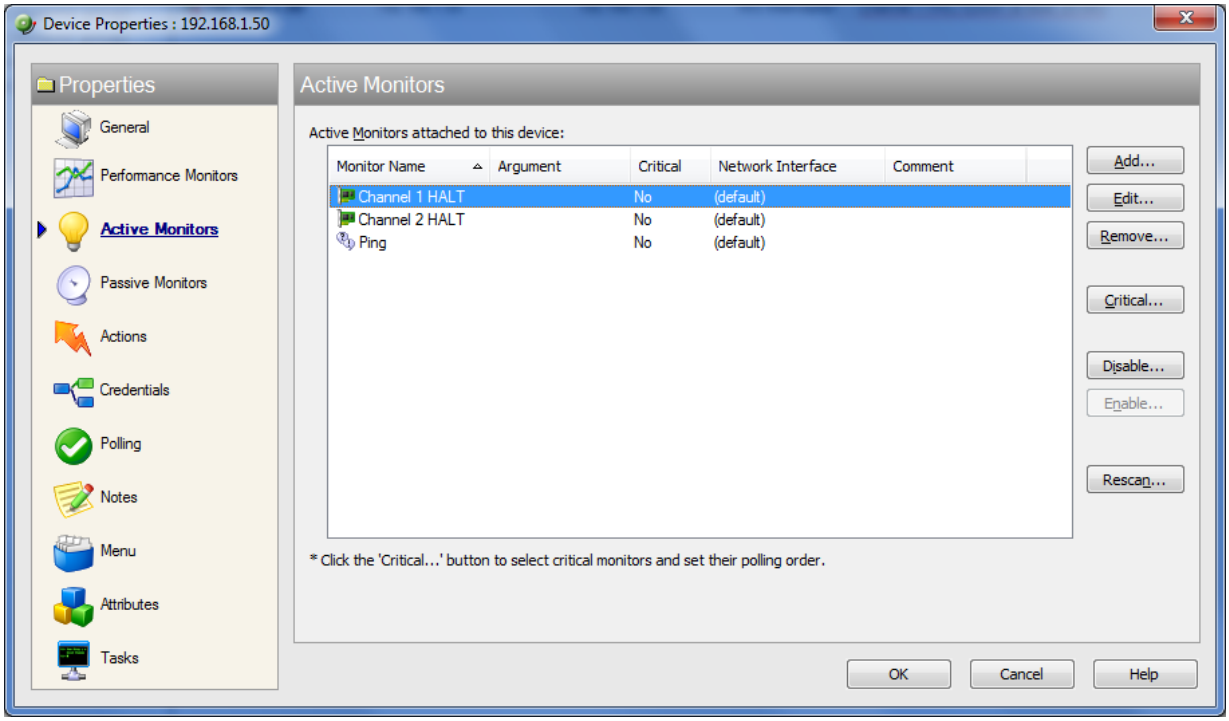


4 Bind Interceptor Active Monitors to IF up/down actions

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...

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

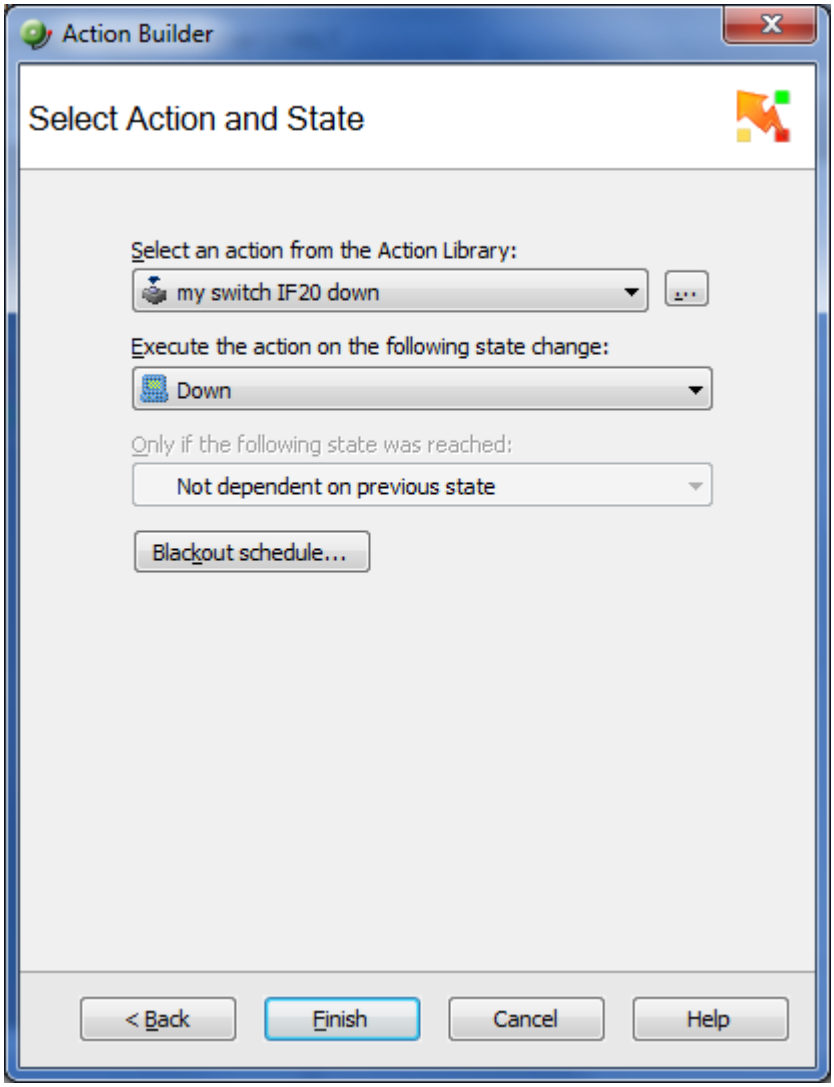
info@networkintegritysystems.com
www.networkintegritysystems.com



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

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

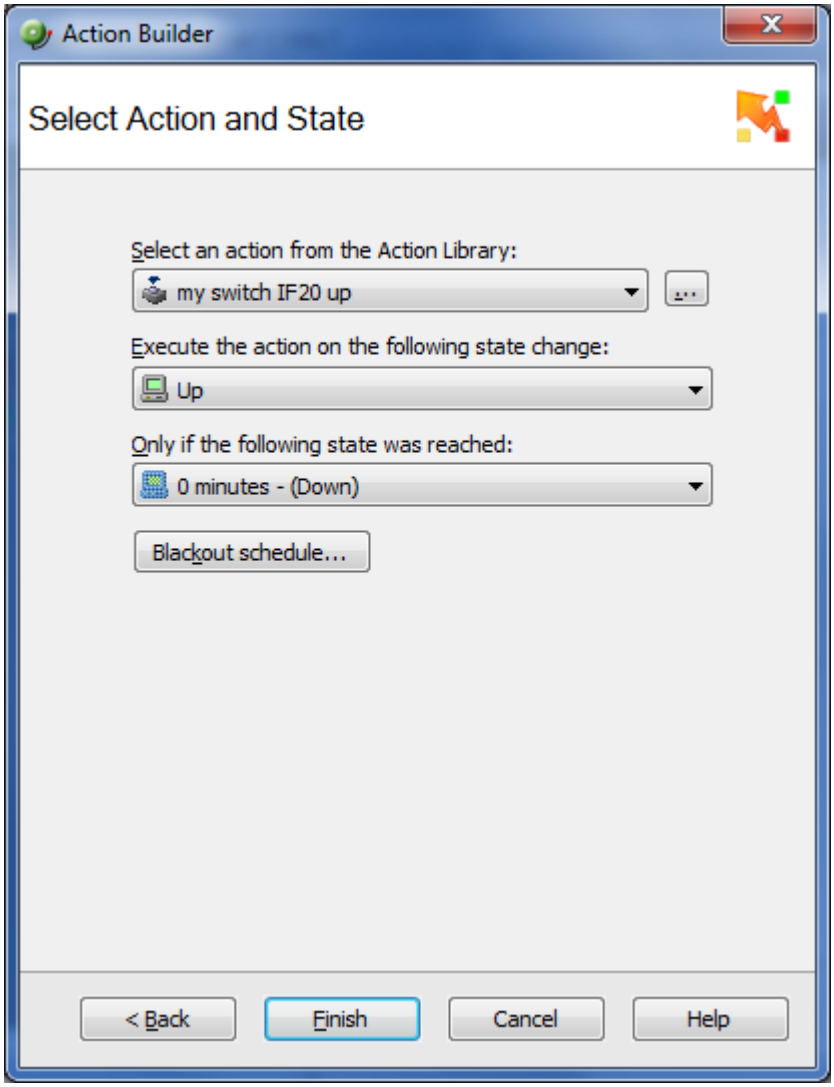
info@networkintegritysystems.com
www.networkintegritysystems.com



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

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

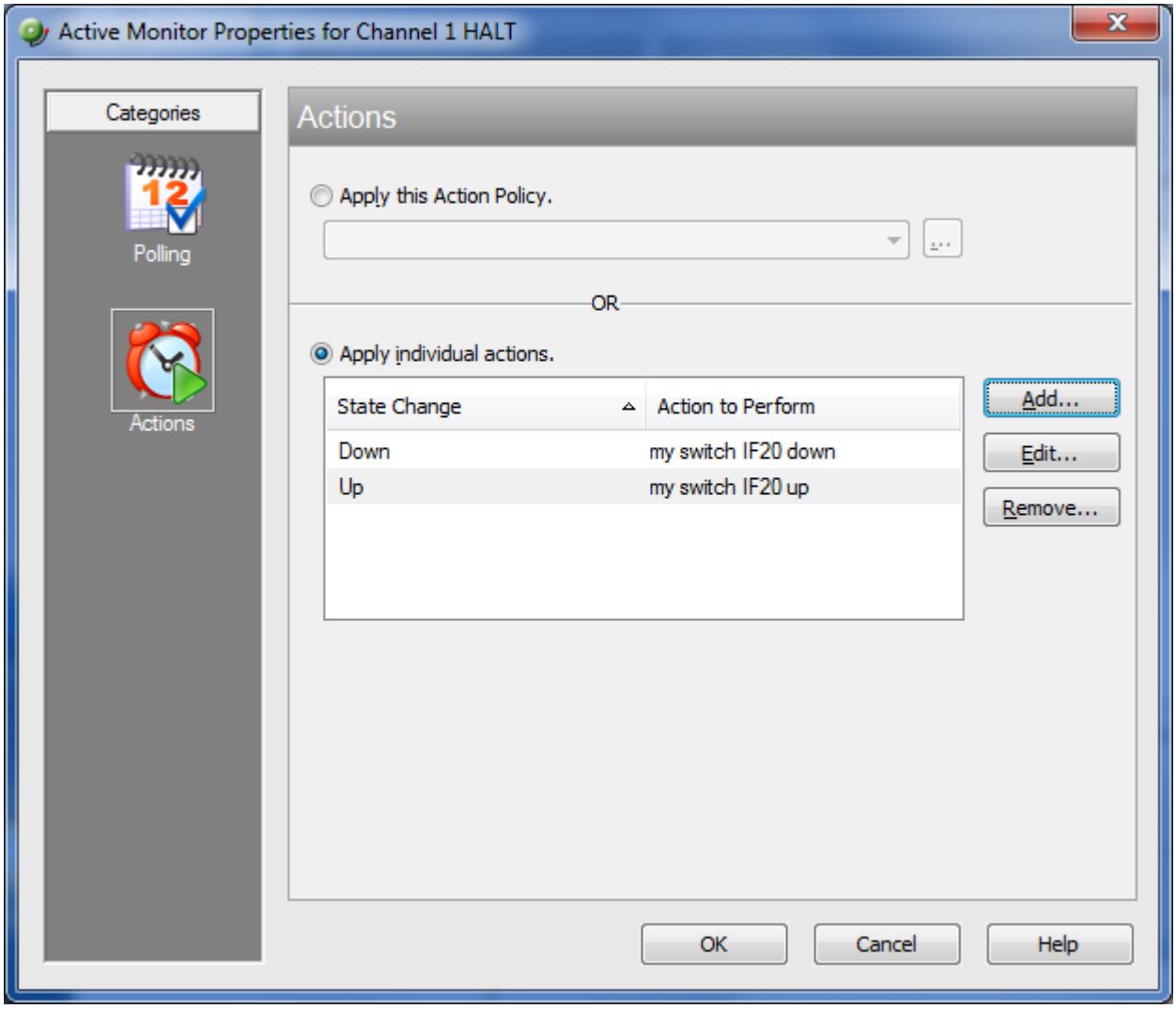
info@networkintegritysystems.com
www.networkintegritysystems.com



The completed action list should appear as follows...

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

info@networkintegritysystems.com
www.networkintegritysystems.com



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

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™