

We Bring Security To Light™

Application Note: Use of Unbrowse SNMP Trap Receiver with Interceptor

The Interceptor has the capability of issuing SNMP Traps upon detecting an intrusion. Several of our users have requested an inexpensive trap receiver application for use with the Interceptor. This application note will detail the setup and use of such a trap receiver, Unbrowse SNMP (<http://www.unleashnetworks.com/unbrowse-snmp-product-page/unbrowse-home.html>)

Obtain MIB's from NIS

Prior to receiving traps with the application, you will need to download the following MIB's (Management Information Base files) from the NIS FTP site. The file names are:

NETWORKINTEGRITYSYSTEMS-GENERALFOIDS-MIB.txt
NETWORKINTEGRITYSYSTEMS-GLOBAL-REG.txt

Download and install Unbrowse SNMP

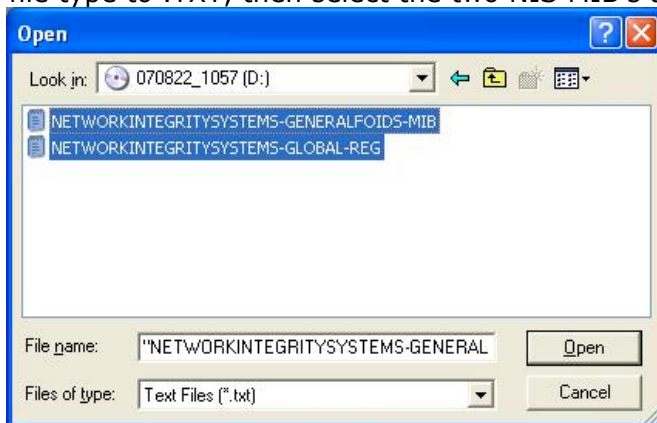
Download and install the Unbrowse SNMP application, accessible from the following link:
<http://www.unleashnetworks.com/unbrowse-snmp-product-page/unbrowse-home.html>

Follow the instructions as indicated in the installation file. Choose "Typical Installation" when prompted.

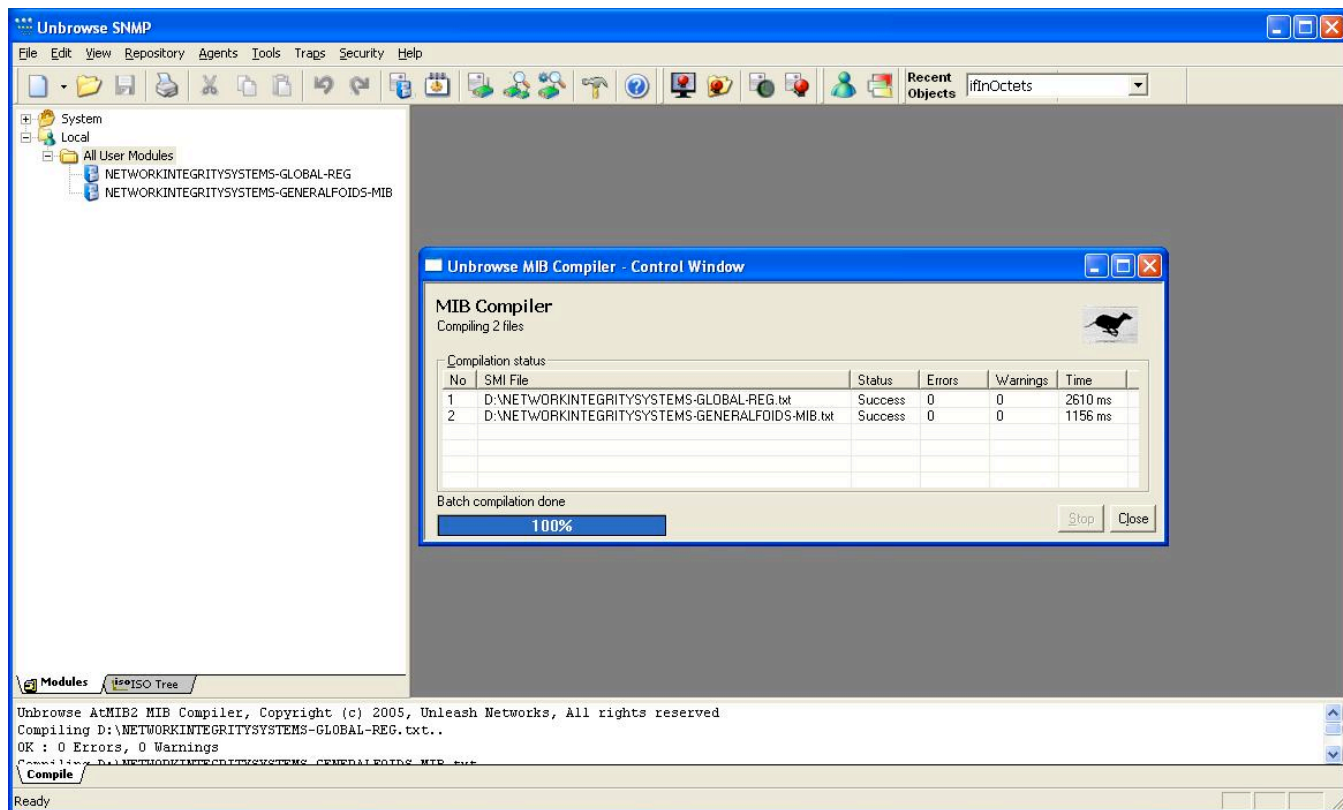
Compile MIB's

The MIB files downloaded from NIS must first be compiled into the Unbrowse SNMP format. Do this as follows:

1. At the main Unbrowse SNMP screen, select Repository/Batch Compile
2. Change the file type to .TXT, then select the two NIS MIB's as shown below:



Press Open; the compiler will then process the MIB's and add them to the Repository.



4. Press Close when the process has completed.

Add Agent

In order for Unbrowse SNMP to recognize the Interceptor, the Interceptor must be added to Unbrowse SNMP as an Agent. Create an Agent as follows:

At the main Unbrowse SNMP screen, select Agents/Manage/Create new Agent. This function appears as a button on the Agents/Manage screen.

Click on the new agent, and select the Edit Selected Agent button. Configure the Agent as shown below:

Agent Name: reference name for this Interceptor in Unbrowse SNMP

IP Address: Address of the Interceptor issuing traps

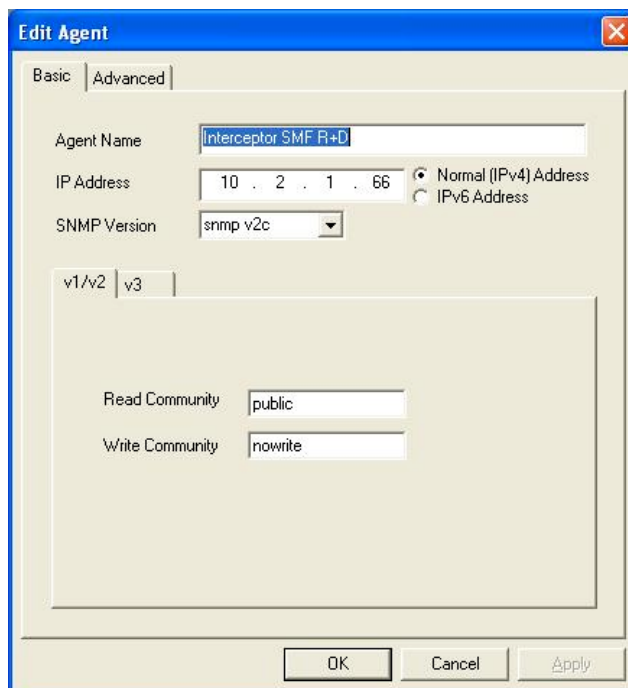
SNMP Version: Version of SNMP you wish to use. NOTE: The Interceptor does not currently have SNMPv1 capability

Read Community: This is the Read "password" used for access to the Interceptor via SNMP. This must match the RO Community String set in the Interceptor SNMP Configuration, and the

We Bring Security To Light™

Target Community String in the Interceptor Alarm Target. Leave this setting as "public" (default) unless you specifically wish to change it for your needs.

Write Community: This is the Read/Write "password" used for access to the Interceptor via SNMP. This must match the RW Community String set in the Interceptor SNMP Configuration. Leave this setting as "nowrite" (default) unless you specifically wish to change it for your needs.



3. Press Ok to enable set features.

Set up Interceptor SNMP Configuration

The SNMP Configuration of the Interceptor (accessed from the main Interceptor screen, under Comms Configuration/SNMP Configuration) must be set up as shown below:

Set sysName as you wish it to appear in the SNMP application

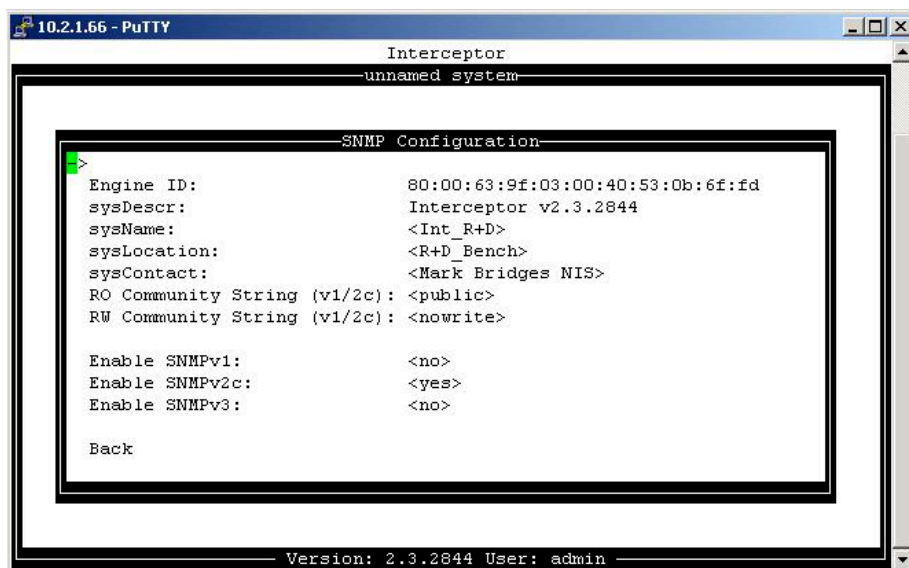
Set sysLocation as you wish it to appear in the SNMP application

Set sysContact as you wish it to appear in the SNMP application

Set the RO Community String to match the Read Community setting in the Agent in the previous example (if default setting for the Read Community in step 2 in Add Agent above was "public", enter it here)

Set the RW Community String to match the Write Community setting in the Agent in the previous example (if default setting for the Write Community in step 2 in Add Agent above was "nowrite", enter it here)

Set Enable SNMPv2c to Yes



Set up Interceptor SNMP Alarm Target

It is necessary to configure an Alarm Target so that the Interceptor will send SNMP Traps to the Trap Receiver. Do this as follows:

In the Interceptor main screen, select Alarm Target Configuration/Add Alarm Target. Enter the name of the Alarm Target (this will be used to identify the Target within the Interceptor).

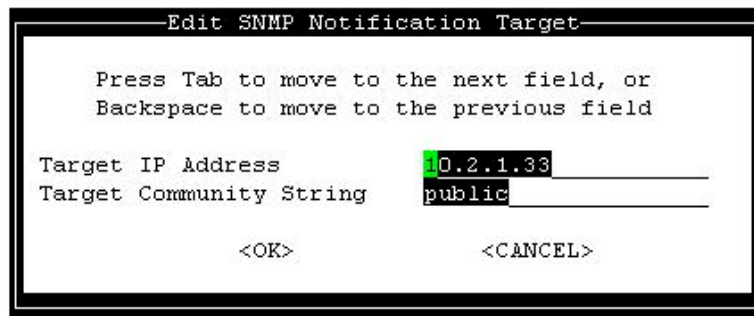
Select SNMP Notification (Trap) from the next menu.

Enter the following information in the Create SNMP Notification Target screen:

Target IP Address: the IP address of the PC with the Unbrowse SNMP application

(NOTE: To find the IP Address of the PC, select Start/Programs/Accessories/Command prompt. Enter "ipconfig" on the command line, and press Enter. The indicated IP Address of the network interface in use will be the IP address entered at this time.)

Target Community String: This "password" must match the Read Community string as set up in the Unbrowse SNMP Agent for the Interceptor (if default setting for the Read Community in step 2 in Add Agent above was "public", enter it here)



We Bring Security To Light™

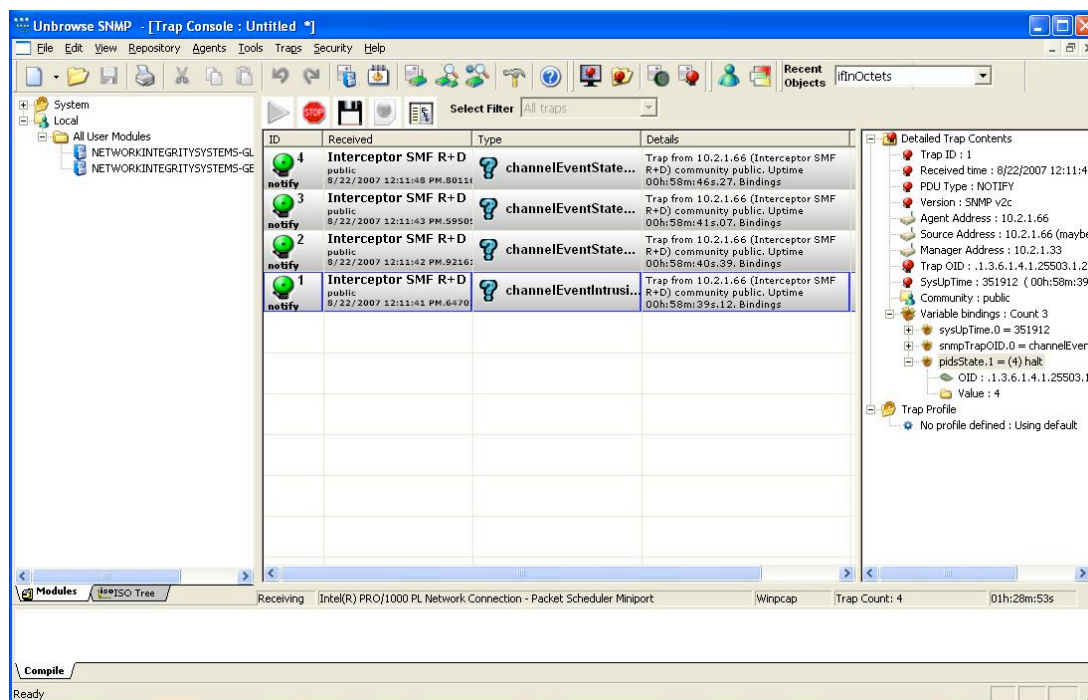
Select OK to finish the Alarm Target setup.

You are now ready to send and receive traps with the Interceptor and Unbrowse SNMP.

Start Trap Reception

In order to receive traps, you will need to enable the Trap Console in Unbrowse SNMP. Enable this function by selecting Traps/New Trap Console. After the Trap Console has started, press the yellow arrow to start receiving Traps.

As traps are received, they will appear as follows:



In this case there were four traps received, the first was an Intrusion trap, and the other three were Event State Change traps issued as the Interceptor was reset. If you wish to view the Detailed Trap Contents window as shown above, press the Show/Hide Trap Details Window selection button at the top of the Trap Window.

NOTE 1: If traps are not received, verify that the proper network interface is specified in the line near the bottom of the Trap Console.

Editing Trap Profile

In Unbrowse SNMP, it is possible to use a received trap to create a Trap Profile, which will then modify the appearance of the same traps in a way that the user specifies. We will use the Trap Profile feature to highlight Event Intrusion traps for greater visibility. NOTE: The specific trap

We Bring Security To Light™

must be visible in the Trap Console before its Trap Profile may be edited. Set up the Trap Profile as follows:

Right click on the channelEventIntrusion trap, and select Define Trap Profile. Select Yes when asked if you wish to create a Trap Profile.

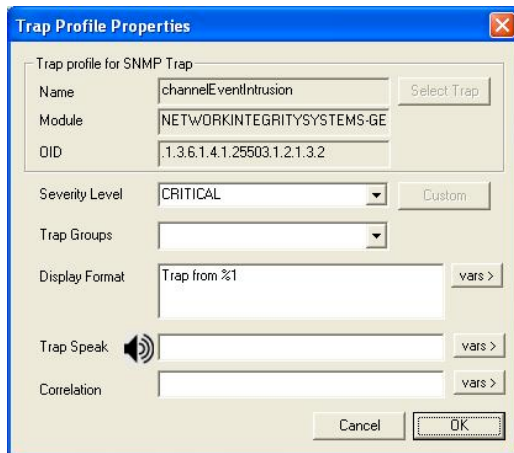
Enter the information fields in the Trap Profile as follows:

Name, Module, OID: Do not change these

Severity Level: Select the level of the trap severity; CRITICAL will highlight the trap in red as shown in our examples

Display Format: Enter as shown below; this will display the pidsState variable, which displays the Interceptor channel that has detected an intrusion

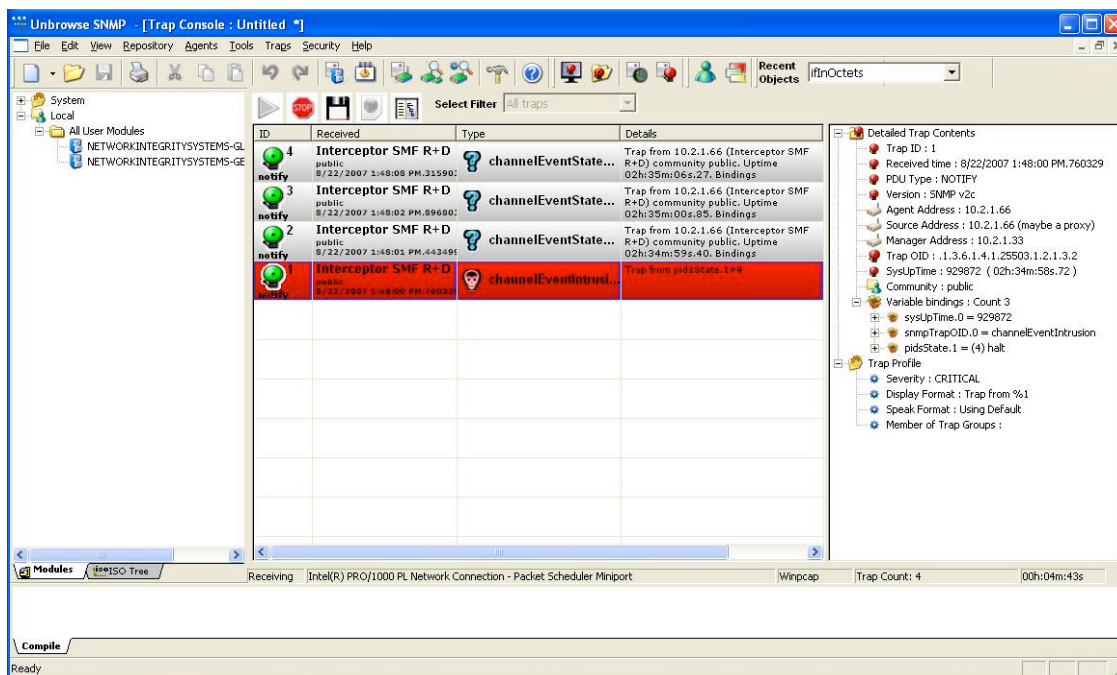
There are other options, such as Trap Speak, which will then give an audible indication (from a user specified .wav file) when a channelEventIntrusion trap is received



The image shows a 'Trap Profile Properties' dialog box. It contains the following fields and controls:

- Name:** channelEventIntrusion
- Module:** NETWORKINTEGRITYSYSTEMS-GE
- OID:** 1.3.6.1.4.1.25503.1.2.1.3.2
- Severity Level:** CRITICAL (with a 'Custom...' button)
- Trap Groups:** (empty dropdown)
- Display Format:** Trap from %1 (with a 'vars >' button)
- Trap Speak:** (with a speaker icon and a 'vars >' button)
- Correlation:** (empty field with a 'vars >' button)
- Buttons:** Cancel and OK

Press OK. The received channelEventIntrusion traps in the Trap Console will change to reflect the entries in the Trap Profile. See the figure below for an example:

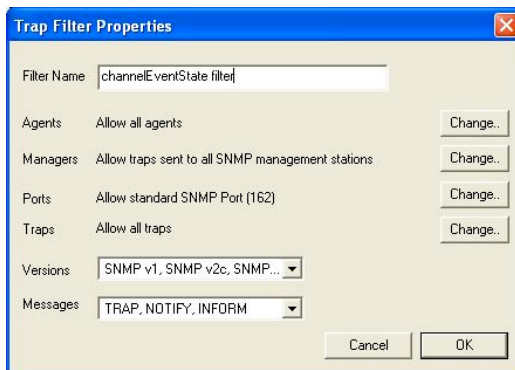


The Intrusion trap is highlighted in red, and in the Details column it can be seen that channel 1 has detected an intrusion (pidsState.1), and the channel is in Halt.

Create a Trap Filter

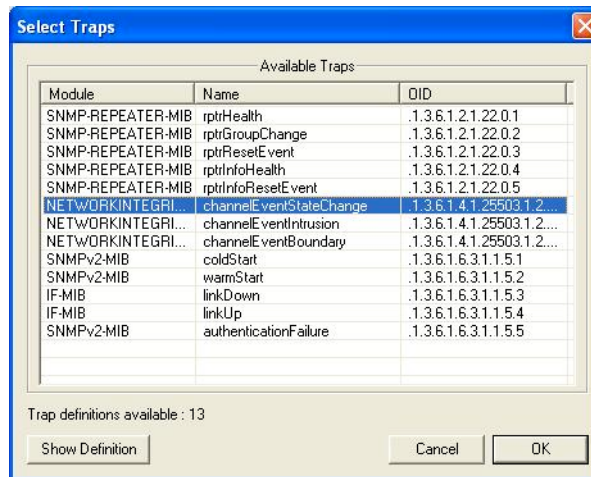
If desired, the user may create a Trap Filter to Unbrowse SNMP that will prevent the channelEventState traps (or any other selected traps) from displaying in the Trap Console. This filter may be created as follows:

- Select Traps/Manage Filters from the main Unbrowse SNMP screen.
- Double click on Create a new SNMP Trap Filter.
- In the Trap Filter Properties screen, enter the following information:
Filter Name: enter the name of the filter

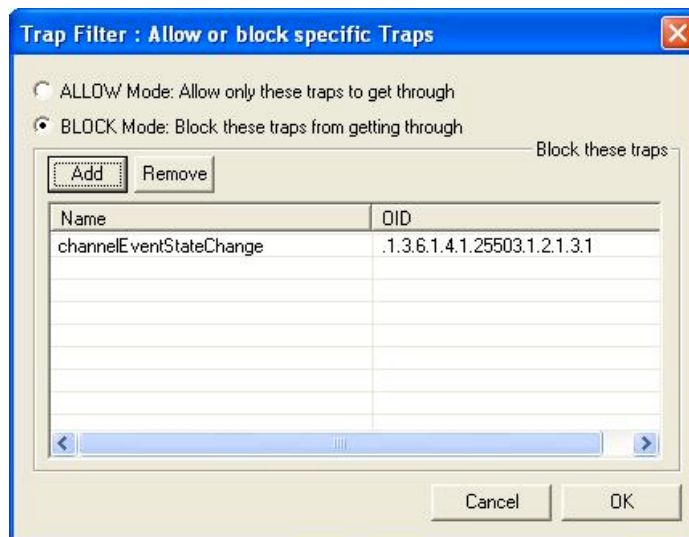


Traps: press Change

in the "Trap Filter: allow or block specific traps" screen press Add. In the Select Traps screen, click on the channelEventStateChange trap (or the trap you wish to filter) as shown below:



Press OK, the Trap Filter screen should reappear with the selected trap to be filtered. Now select BLOCK Mode as shown below:

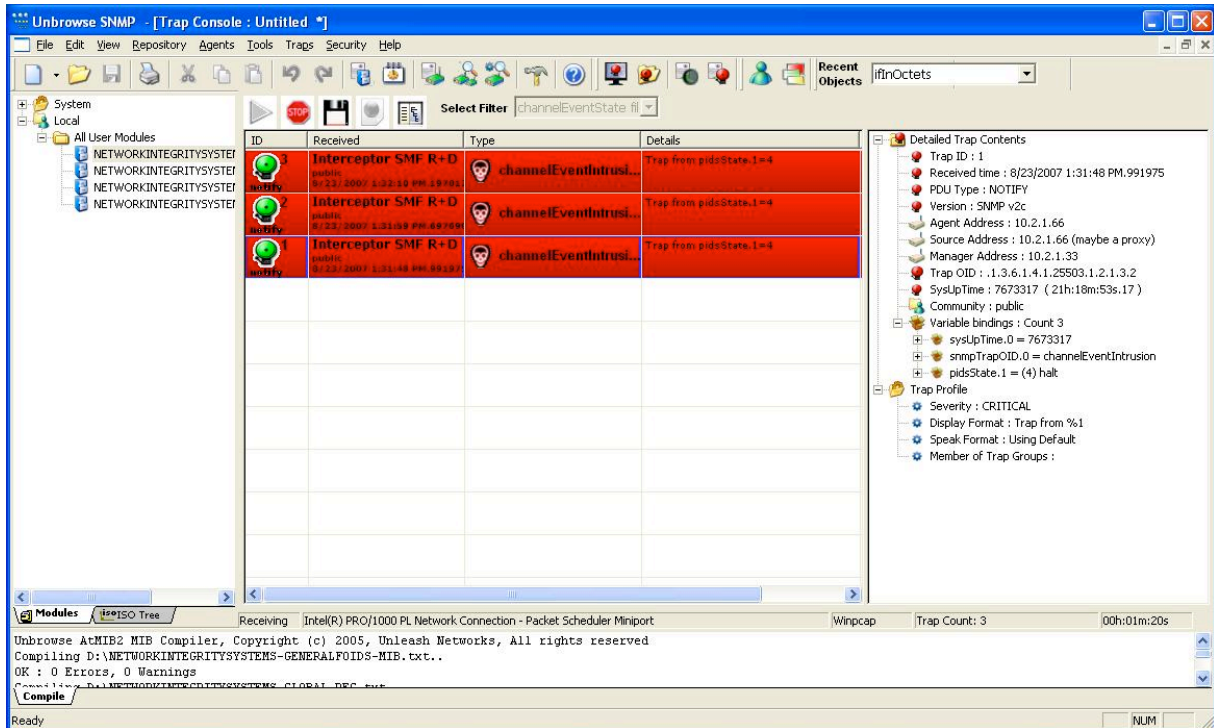


Press OK three times to complete the filter setup.

When the Trap Console is restarted, select the Trap Filter you just created from the Select Filter selection button at the top of the Console screen (you will also need to stop trap reception in order to make this selection by pressing the Stop the Trap Console button at the top of the Console screen). The traps selected in the Trap Filter will then not be displayed in the Console

We Bring Security To Light™

screen. In the following screen, the channelEventStateChange traps are filtered, only allowing intrusion traps from the Interceptor to be displayed on the Trap Console:



IMPORTANT NOTE:

In order for Unbrowse SNMP to receive traps in most cases, you must disable any antivirus software (such as Norton Antivirus or Windows Firewall) on the host PC.