

info@networkintegritysystems.com www.networkintegritysystems.com

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: <a href="http://www.unleashnetworks.com/unbrowse-snmp-product-page/unbrowse-home.html">http://www.unleashnetworks.com/unbrowse-snmp-product-page/unbrowse-home.html</a>

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:





info@networkintegritysystems.com www.networkintegritysystems.com

We Bring Security To Light<sup>™</sup>

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

W Unbrowse SNMP						
Eile Edit Yiew Repository Agents Tools Traps Security He	lp					
□ · ▷ □  □ · ▷ □  □ · ▷ □	. 🛎 😼 🍣 👕 🥑 🖳 🖗 🖕	🚴 🛃 🖪	ecent bjects	ifInOctets		
System						
	Unbrowse MIB Compiler - Control Window					
	MIB Compiler Compiling 2 Files				*	
	Compilation status	Status	Errors	Warnings	Time 1	
	1 D:\NETWORKINTEGRITYSYSTEMS-GLOBAL-REG.txt 2 D:\NETWORKINTEGRITYSYSTEMS-GENERALFOIDS-MIB.txt	Success Success	0	0 0	2610 ms 1156 ms	
	Batch compilation done					
\∰ Modules ∫ui≠o150 Tree /						
Unbrowse AtMIB2 MIB Compiler, Copyright (c) 2005, Compiling D:\NETWORKINTEGRITYSYSTEMS-GLOBAL-REG. OK : O Errors, O Warnings	Unleash Networks, All rights reserved xt					
Compile						
Ready						

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



info@networkintegritysystems.com www.networkintegritysystems.com

#### We Bring Security To Light<sup>™</sup>

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.

Sasic Advanced	
Agent Name	Interceptor SMF R+D
IP Address	10 . 2 . 1 . 66 • Normal (IPv4) Address
SNMP Version	snmp v2c 🔹
Read Com	munity public
Write Comr	munity nowrite

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



info@networkintegritysystems.com www.networkintegritysystems.com

We Bring Security To Light™

1.66 - PuTTY		
I	nterceptor	
unn	amed system	
SNMP	Configuration	
>		
Engine ID:	80:00:63:9I:03:00:40:53:0b:6I:Id	
sysDescr:	Interceptor v2.3.2844	
sysName:	<int_r+d></int_r+d>	
sysLocation:	<r+d_bench></r+d_bench>	
sysContact:	<mark bridges="" nis=""></mark>	
RO Community String (v1/2c):	<public></public>	
RW Community String (v1/2c):	<nowrite></nowrite>	L
Enable SNMPv1:	<no></no>	L
Enable SNMPv2c:	<yes></yes>	
Enable SNMPv3:	<no></no>	L
Back		I
Version: 2	.3.2844 User: admin	

### 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)

Press Tak	) to move to	the next field, or
Backspace	e to move to	the previous field
Target Commun	nity String	public
	<ok></ok>	<cancel></cancel>

AN-107/June 2011



info@networkintegritysystems.com www.networkintegritysystems.com

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.

*** Unbrowse SNMP - ITrap Console : Ur	titled *1				
Eile Edit View Repository Agents Tool	; Traps 😫	ecurity <u>H</u> elp			
0.0000000000000000000000000000000000000	19 (24	1 🔂 🍯	§ ବ 🞯 🖳 🐑	🐞 💱 🚴 🛃 Recent Objects	finOctets 💽
E System	50	E Sele	ect Filter All traps		
Al User Modules     NETWORKINTEGRITYSYSTEMS-GL     NETWORKINTEGRITYSYSTEMS-GE	ID 4 notify	Received Interceptor SMF R+D public 8/22/2007 12:11:48 PM.80110	Type	Details Trap from 10.2.1.66 (Interceptor SMF R+D) community public. Uptime 00h:58m:46s.27, Bindings	Detailed Trap Contents     P Trap ID : 1     Received time : 8/22/2007 12:11:41     DULTure 1 MOTEN
	2 <sup>3</sup>	Interceptor SMF R+D public 8/22/2007 12:11:43 PM.5950	💡 channelEventState	Trap from 10.2.1.66 (Interceptor SMF R+D) community public. Uptime 00h:58m:41s.07. Bindings	Version : SNMP v2c     Jagent Address : 10.2.1.66
	2 netify	Interceptor SMF R+D public 8/22/2007 12:11:42 PM.9216:	💡 channelEventState	Trap from 10.2.1.66 (Interceptor SMF R+D) community public. Uptime 00h:58m:40s.39. Bindings	<ul> <li>Source Address : 10.2.1.66 (maybe</li> <li>Manager Address : 10.2.1.33</li> <li>Tran OID : .1.3.6.1.4.1.25503.1.2.</li> </ul>
	21 notify	Interceptor SMF R+D public 8/22/2007 12:11:41 PM.6470	💡 channelEventIntrusi	Trap from 10.2.1.66 (Interceptor SMF R+D) community public. Uptime 00h:58m:39s.12. Bindings	SysUpTime : 351912 (00h:58m:39:     SysUpTime : upblic
					→ Value : 4 → ク Trap Profile → ◇ No profile defined : Using default
					_
Ag Modules / USO Tree /	<		Transition - Dealert Calendary Mari		
	Receiving	Intel(R) PRO/1000 PL Network (	Lonnection - Macket Scheduler Minip	winpcap i	rap Counc: 4 U1h:28m:53s
\_Compile_					
Ready					

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 AN-107/June 2011 April 18, 2012 5



info@networkintegritysystems.com www.networkintegritysystems.com

#### 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

Trap Profile Prop	perties	
Trap profile for SN	MP Trap	
Name	channelE ventIntrusion	Select Trap
Module	NETWORKINTEGRITYSYSTEMS-GE	
OID	.1.3.6.1.4.1.25503.1.2.1.3.2	
Severity Level		Custom
Trap Groups	·	
Display Format	Trap from %1	vars >
Trap Speak 📢		vars >
Correlation		vars >
	Cancel	

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:



info@networkintegritysystems.com www.networkintegritysystems.com

We Bring Security To Light<sup>™</sup>

🛄 Unbrowse SNMP - [Trap Console : Untitled *]					
Eile Edit View Repository Agents Tools	Traps	Security Help		_ 8 ×	
	19 (	*   🔁 😃 🍣 🍣   🛜 🕑   🖳 👀	) 🔯 🔏 🖪 Recent ifind	Detets	
System     System     All User Modules     All User Modules     NETWORKINTEGRITYSYSTEMS-GL     NETWORKINTEGRITYSYSTEMS-GE	ID ID ID ID ID ID ID ID ID ID	Necetived     Type     Deta       Interceptor SMF R+D public     Type     Received	als o from 10.2.1.66 (Interceptor SMF ) community public. Uptime 135mn06s.27. Bindings o from 10.2.1.66 (Interceptor SMF ) community public. Uptime		
	notify 2 notify	6/22/2007 1:48:02 PM.89680: 02h: Interceptor SMF R+D public 8/22/2007 1:48:01 PM.443495 8/22/2007 1:48:01 PM.443495 8/22/2007 1:48:01 PM.443495 8/22/2007 1:48:01 PM.496800 8/22/2007 1:48:01 PM.896800 8/22/2007 1:48:01 PM.496800 8/22/2007 1:48:0000 8/22/2007 1:48:000000 8/22/2007 1:48:00000000000000000000000000000000000	: 35m:00s.85. Bindings o from 10.2.1.66 (Interceptor SMF )) community public. Uptime : 34m:59s.40. Bindings	Source Address : 10.2.1.66 (maybe a proxy) Manager Address : 10.2.1.33 Trap OID : 1.3.6.1.4.1.25503.1.2.1.3.2	
		Interceptor SMF R+D assu- b/22/2007 SHI (00 eM / 2003)	- teren politikana, kon	<ul> <li>SystJpTime : 929972 (02h:34m:58s.72)</li> <li>Commarky : public</li> <li>Variable bindings : Count 3</li> <li>SystJpTime : 929872</li> <li>SystJpTime : 1491</li> <li>Severity : CRITICAL</li> <li< td=""></li<></ul>	
Modules Jeso Tree	eceiving	Intel(R) PRO(1000 PL Network Connection - Packet Scheduler Mininort	Winncan	Tran Count: 4 00b:04m:43s	
Compile /		proegry nograder i i norman den fielden i færse den boden i miljøre.			

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

Filter Name	channelE ventState filter	
Agents	Allow all agents	Change.
Managers	Allow traps sent to all SNMP management stations	Change.
⊃orts	Allow standard SNMP Port (162)	Change.
Traps	Allow all traps	Change.
Versions	SNMP v1, SNMP v2c, SNMP 💌	
Messages		



info@networkintegritysystems.com www.networkintegritysystems.com

We Bring Security To Light<sup>™</sup>

#### 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:

Module	Name	OID
SNMP-REPEATER-MIB	rptrHealth	.1.3.6.1.2.1.22.0.1
SNMP-REPEATER-MIB	rptrGroupChange	.1.3.6.1.2.1.22.0.2
SNMP-REPEATER-MIB	rptrResetEvent	.1.3.6.1.2.1.22.0.3
SNMP-REPEATER-MIB	rptrInfoHealth	.1.3.6.1.2.1.22.0.4
SNMP-REPEATER-MIB	rptrInfoResetEvent	.1.3.6.1.2.1.22.0.5
NETWORKINTEGRI	channelEventStateChange	.1.3.6.1.4.1.25503.1.2
NETWORKINTEGRI	channelE ventIntrusion	.1.3.6.1.4.1.25503.1.2
NETWORKINTEGRI	channelEventBoundary	.1.3.6.1.4.1.25503.1.2
SNMPv2-MIB	coldStart	.1.3.6.1.6.3.1.1.5.1
SNMPv2-MIB	warmStart	.1.3.6.1.6.3.1.1.5.2
IF-MIB	linkDown	.1.3.6.1.6.3.1.1.5.3
IF-MIB	linkUp	.1.3.6.1.6.3.1.1.5.4
SNMPv2-MIB	authenticationFailure	.1.3.6.1.6.3.1.1.5.5

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

Trap Filter : Allow or block spec	ific Traps 🛛 🔀
ALLOW Mode: Allow only these trap     BLOCK Mode: Block these traps from	s to get through n aettina through
Add Remove	Block these traps
Name	OID
channelE ventStateChange	.1.3.6.1.4.1.25503.1.2.1.3.1
	Cancel DK

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



info@networkintegritysystems.com www.networkintegritysystems.com

#### We Bring Security To Light<sup>™</sup>

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

*** Unbrowse SNMP - [Trap Console	: Untitleo	d *]			
Elle Edit View Repository Agents	<u>T</u> ools Tra	ps <u>S</u> ecurity <u>H</u> elp			- 8 ×
	6 9	P 🖥 🖥 🍓	8 🌮 🕘 🖳	😰 🐞 🦆 🚴 📇 Recent Objects	ifInOctets 🔹
E System	D 10	🕨 💾 💌 🔣 Sele	ect Filter  channelEventState f		
All User Modules	ID	Received	Туре	Details	🖃 🍓 Detailed Trap Contents
NETWORKINTEGRITYSYSTEF		Interceptor SMF R+D public Br23/2007 1:32:10 PM 19701	General Channel EventIntrusi.	Trap from pidsState.1=4	Prap ID : 1     Pg Received time : 8/23/2007 1:31:48 PM.991975     PDLI Type : NOTIEV
	<b>@</b> 2	Interceptor SMF R+D public 8/23/2007 1:31:59 PM.697690	🗑 channelEventIntrusi.	Trap from pidsState.1=4	- 🖗 Version : SNMP v2c 
	<b>@</b>	Interceptor SMF R+D public 0/23/2007 1:31:48 PHI.99197	🗑 channelEventIntrusi.	Trap from pidsState.1=4	Source Address : 10.2.1.66 (maybe a proxy) Manager Address : 10.2.1.33 Tran OID : 1.3.6.1.4.1.25503.1.2.1.3.2
< >					<ul> <li>SysUpTime: 7673317 (21h:18m:53s.17)</li> <li>Community: public</li> <li>Warlabe bindings: Count 3</li> <li>sysUpTime.0 = 7673317</li> <li>sysUpTime.0 = 7673317</li> <li>sysUpTime.0 = channelizentIntrusion</li> <li>pidsState.1 = (4) halt</li> <li>Trap Profile</li> <li>Display Format: 1: (4) halt</li> <li>Speak Format: 1: Using Default</li> <li>Member of Trap Groups:</li> </ul>
Modules Deres	Receiving	Intel(R) PRO/1000 PL Network (	Connection - Packet Scheduler Mini	port Winpo	ap Trap Count: 3 00h:01m:20s
Unbrowse AtMIB2 MIB Compiler, C Compiling D:\NETWORKINTEGRITYSY OK: 0 Errors, 0 Warnings Compile	opyright STEMS-GEN STEMS CLO	(c) 2005, Unleash Netw MERALFOIDS-MIB.txt	rorks, All rights reserv	ed	
Ready					NUM

#### 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.