

NetSight Atlas Console 1.5

Automated Security Manager 1.1

Activity Monitor Troubleshooting Guide

Introduction

This guide can help the first time user of ASM solve basic configuration problems associated with receiving SNMPv3 Informs and triggering ASM's response to potential network threats. Begin by using the ASM Activity Monitor Troubleshooting Chart. It covers key items that can be verified when incidents do not appear in the ASM Activity Monitor.

The Basics

ASM will not be usable unless you have at least created a database of Network Elements. At the very least, you need to discover or import the devices that you want to protect with DIRS. The care you take creating an accurate database of your network elements, the more efficiently ASM can be used to search and isolate threats.

1. **Define Device Groups:** Although Console has many predefined folders, it would be easier defining Search Scopes in the long run, if you take the time upfront to create Device Groups for the network in question. For instance, you could organize your network Elements by geographic region, Data Center, DMZ and Access Devices to name a few.

See the Help Documentation for Network Elements on how to create Device groups. Drag and drop devices in these new folders in a way that makes sense for your organization. This might be by geographic location, building, floor or use as in edge device, datacenter, DMZ, etc.

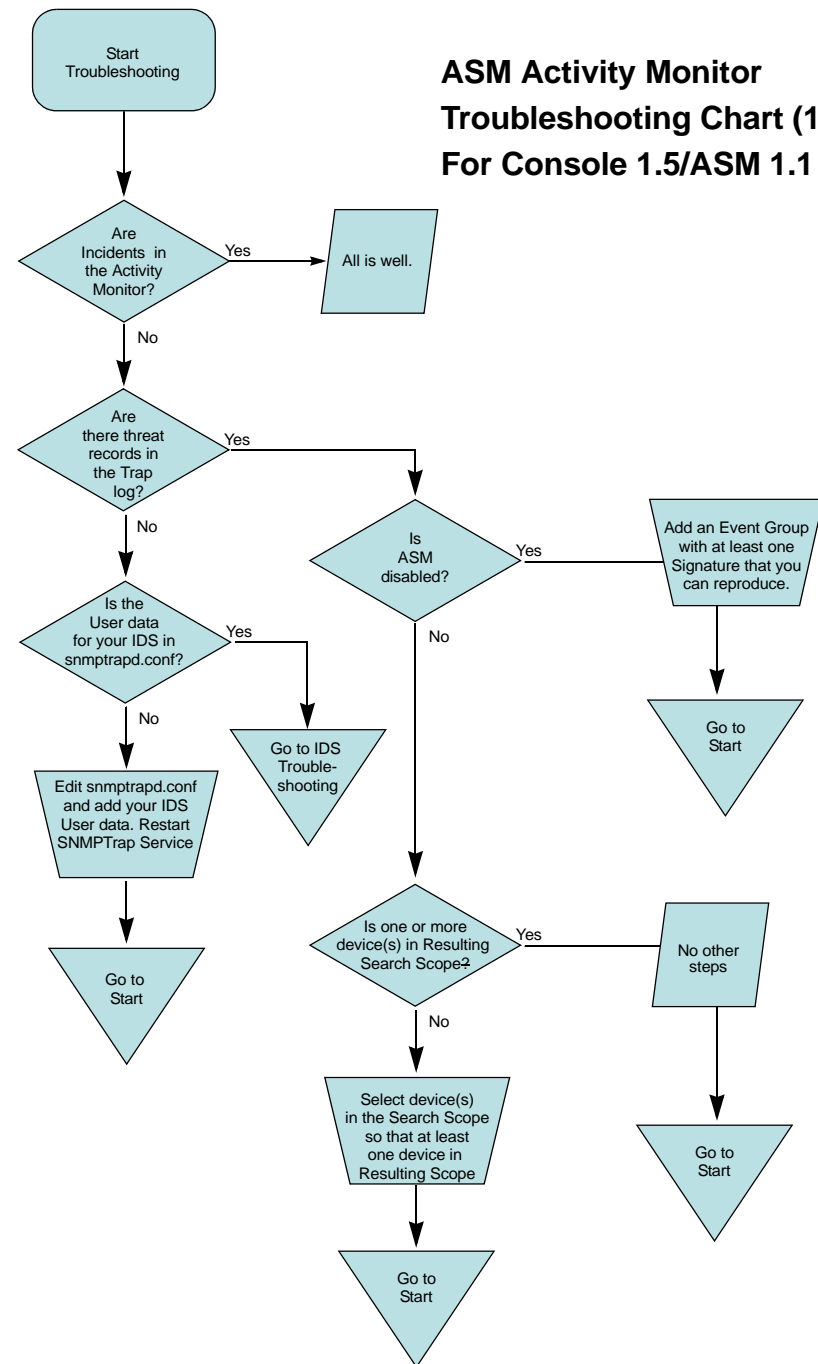
2. **Configure SNMPTrap Service:** The snmptrapd service that is provided with NetSight Atlas Console / ASM will need to be configured to prepare ASM for receiving Informs from one or more Dragon IDS servers.

You will need to edit the configuration file `snmptrapd.conf` which is located in the `<install dir>\NetSight Atlas Console\bin` directory.

Note: The easiest way to configure the SNMPv3 user credentials in the `snmptrapd.conf` file is by using a text editor.

In a Windows environment, right-click the Atlas Services Manager Icon and select **SNMPTrap > Configure** to open a text editor where you can edit the `snmptrapd.conf` file.

ASM Activity Monitor Troubleshooting Chart (1) For Console 1.5/ASM 1.1



Initially, this file is just commented text that explains how to enter a SNMPv3 credential and gives an example. For Dragon IDS to send DIRS threat informs, user credentials must be entered that will match a user's credentials for a given Dragon IDS.

Example:

```
createUser myAuthPrivUser MD5 myauthpassword DES
myprivpassword
```

Where:

- myAuthPrivUser - security user name
- MD5 - authentication type (MD5 or SHA)
- myauthpassword - authentication password (optional parameter - not needed when authentication type is not specified)
- DES - encryption type
- myprivpassword - encryption password - (optional parameter - do not use when encryption is not used or leave the encryption password blank if it is the same as the authentication password).

The variables that need to match at each end, Atlas Console/ASM and Dragon are myAuthPrivUser, myauthpassword, and myprivpassword. Create a new line without the # comment character and provide your own credential information in place of the sample variable.

After saving the `snmptrapd.conf` file, SNMPTrap Service must be restarted so that the updated user information can be learned.

3. Restart the SNMPTrap Service.

Windows	Solaris, Linux
<ol style="list-style-type: none"> 1. Go to the Taskbar Notification Area of your desMktop (on the lower right of your screen, unless you've relocated your Taskbar). 2. Locate the Services Manager icon () and right-click it. 3. Select SNMP Trap > Restart. 	<ol style="list-style-type: none"> 1. Navigate to the <code>etc/rc2.d</code> directory. 2. Type the command: <code>S99NsSnmptrapd stop</code> 3. Press Enter. 4. Type the command: <code>S99NsSnmptrapd start</code> 5. Press Enter.

4. **Configure Dragon IDS Informs:** The latest version of Dragon IDS (6.3) and subsequent releases support DIRS by making it easy to define Notification rules used to alert ASM of potential threats on your network. This step provides an overview showing you where to look later, when you are setting up your own DIRS solution. Refer to the ***Dragon IDS AlarmTool Step-by-Step Instructions*** for more detailed instructions on configuring Dragon IDS to listen for threats and send the threat notifications to ASM.

- a. In Dragon IDS, there are three Alarm Tool options that you must configure: **Event Groups**, **Notification Rules**, and **Alarms**. Configure and **Save** each option:
 - **Event Groups** let you place threat signatures in categories of your choice. For instance, you can choose to create an Event Group called *Really Bad Hack* to collect the threat signature(s) that fall into this category. Dragon provides 15 pre-defined categories of signatures. You can select one or more to associate with a given event group.
 - **Notification Rules** define the other half of the SNMPv3 informs. You will want to create one of these for each of the pre-defined ASM Categories. These pre-defined categories match the predefined ASM Event Categories.

Example:

```
Rule Name:           [note-rule-ATTACKS]
Time Period:         [None]
Server:              <yourConsoleASM-IP>
Security Name:       [<SNMPv3 username>]
Auth PW:             <Auth Password>
Priv PW:             <Private password>
ASM Category:        [ASM_ATTACKS]
```

Note: SNMPv3 parameters given here must match those configured in the Console/ASM `snmptrapd.conf` file. You can use the same SNMPv3 parameters for each of the Notification Rules that you create.

- **ALARMS** tie the Event Groups to Notification Rules to create the Inform message that will be sent to Console/ASM when a signature is detected on the network being protected.

Note: For sending Informs to ASM, the only fields you should be concerned with are: Type: [Real Time], Event Group: [*Really_Bad_Hack*], and Notification Rule:, [*note-rule-ATTACKS*].

b. Select **DEPLOYMENT** and click **Deploy** under **ALARMTOOL CONFIGURATION**.

ARE YOU GETTING TRAPS?

Now that you've configured your SNMPTrap Service and created the GROUP(s), NOTIFICATION(s) and ALARMS on Dragon, you should be able to see if traps can be successfully received in you Console/ASM [Trap] log.

Trap Notification happens when Dragon IDS identifies a traffic signature that matches one of the signatures that you included into your Alarm categories. If you've configured Dragon to look only for viruses or other rare attacks, you may never see a trap (if you're lucky). So for this test, we'll include a signature for an event that is easy for you to produce. When you trigger your test event, you should see traps in the ASM Activity Monitor. Once you can run this test successfully, you can go on to verify other rules that you've created in ASM.

1. In the **Dragon AlarmTool**, add a signature **SNMP:public** from the **PROBE** category to a test **Event Group** called *Really_Bad_Hack*, Save and Deploy the Alarm configuration.

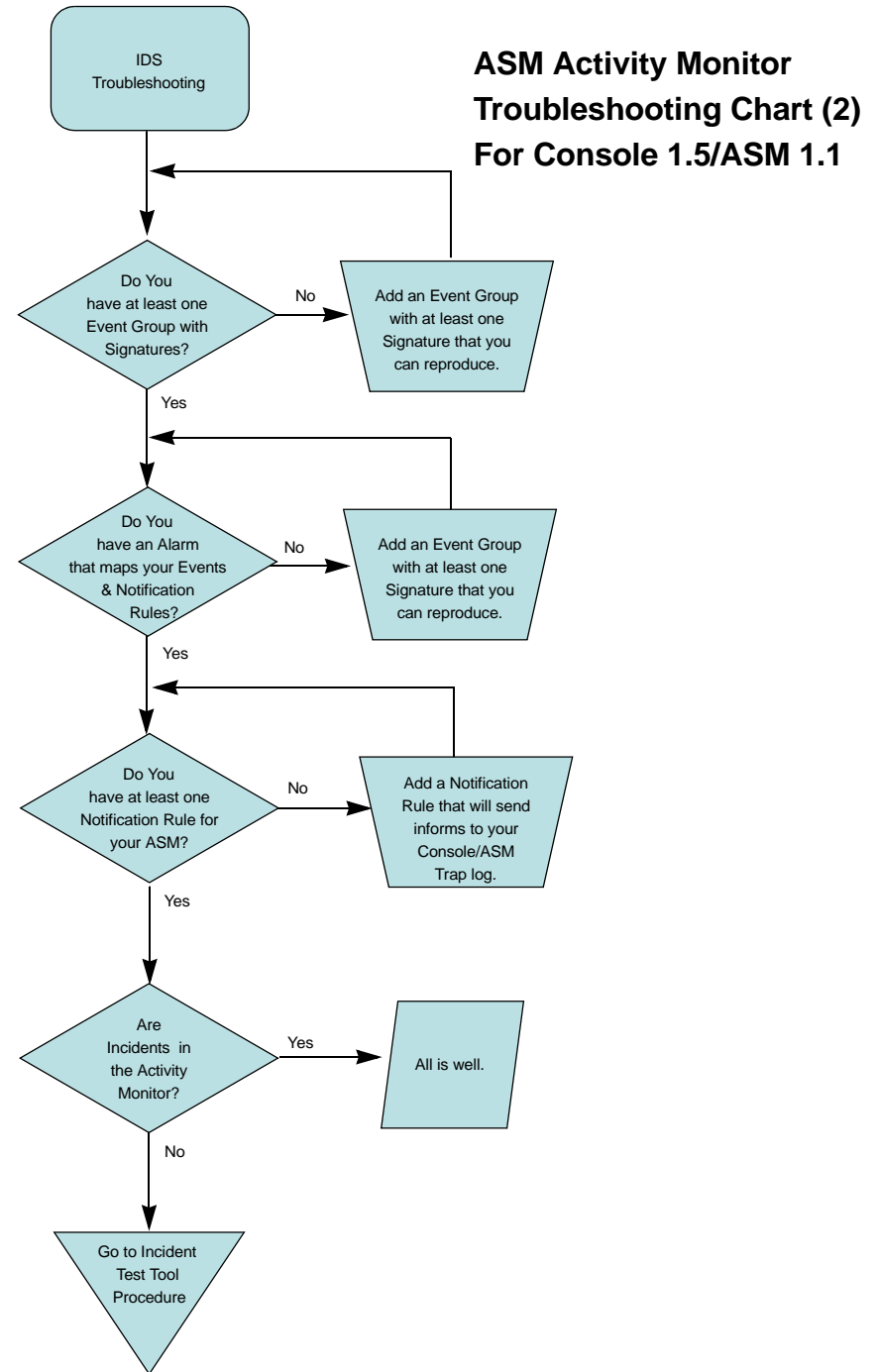
Now, any SNMP traffic using a **public** community name on the network being watched by this Dragon IDS will trigger an SNMP inform to be sent to Console/ASM and Traps/Informs will start appearing in Console's TRAP log. But, ASM cannot act on these inform messages until you configure an appropriate Rule within ASM.

2. **ASM Rule Configuration:** In ASM, begin by defining a basic rule that will start ASM evaluating the incoming Inform messages. Later you can create more complex rule definitions that deal with real threats.
 - a. Open the **Rule Configuration** wizard and define a rule with the search scope to includes one or more devices that typically generate SNMP traffic using the **public** community name.
 - b. Accept the default settings for the rest of the wizard's views and **Save** and **Close** the wizard.
 - c. In the ASM Activity Monitor, set ASM for **Search** or **Search and Respond**.

ASM should now begin evaluating Inform messages from your IDS and you should see incidents in the Activity Monitor.

4. **Fine Tune:** To take action on actual threats you will have to use the ASM Rule Configuration wizard to create more comprehensive rules, capable of applying specific responses to the real threats.

You can also define ASM Options to fine tune Event Categories, Sender IDs, Policies, Action Limits and MIBs to use in the searches.



INCIDENT TEST TOOL

Refer to the Help documentation for information on the Incident Test Tool. This tool lets you test and debug the search scopes and actions to verify ASM's response to an event. You can perform a basic test that sends an inform message directly to ASM, bypassing the SNMPTrap Service, or you can configure a more comprehensive test to test the complete path (IDS to SNMPTrap Service/Console to ASM), simulating exactly the workings of an actual inform message.

To access the Incident Test Tool, click the Test button in the ASM Activity Monitor.