

RSA NetWitness Logs

Event Source Log Configuration Guide



Extreme Networks Dragon IPS

Last Modified: Thursday, July 20, 2017

Event Source Product Information:

Vendor: [Extreme Networks](#)

Event Source: Extreme Networks Dragon IPS (Formerly known as Enterasys Dragon)

Versions: 5.x, 6.x, 7.2, 7.4

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: dragonids

Collection Method: SNMP

Event Source Class.Subclass: Security.IDS

To configure the Extreme Networks Dragon IPS event source, you must:

- I. Configure the Extreme Networks Dragon IPS event source
- II. Configure RSA NetWitness Suite for SNMP Collection

Configure Extreme Networks Dragon IPS

Depending on your version, see one of the following procedures:

- Configure Dragon version 7.2 or 7.4
- Configure Dragon version 5.x or 6.x

Configure Dragon version 7.2 or 7.4

To set up Dragon 7.2 or 7.4:

1. Connect to the EMS Client using administrative credentials.
2. Go to **AlarmTool Policy View**.
3. Expand the **Custom Policies** folder and select an Alarm Tool Policy that you have already created, or, if you have not created one, add an Alarm Tool Policy.
4. On the **Notification Rules** tab, click **New**.
5. In the Edit Notification Tool window, follow these steps:
 - a. In the **Name** field, type **NW-SNMP**.
 - b. In the **Time Period** field, type **None**.
6. Select the new notification rule from the left pane. In the right pane, select the **SNMP V1** tab.
7. Click **New**, and, in the SNMP V1 Editor, complete the fields as follows.

Field	Value
Transport	Type UDP
Server	Enter the IP address of the RSA NetWitness Suite Log Collector.
Port	162
OID	.1.3.6.1.4.1.4471
Trap Type	6

Field	Value
Specific Type	0
Community	public
Message	%ALERT% %SENSOR% %SIP% %DIP% %SPORT% %DPORT% %PROTO% %DIR% %NAME% %DATE% %TIME% %DATA%

8. Click **OK > Commit**.
9. On the **Alarms** tab, click **New**.
10. In the Alarm Editor window, complete the fields as follows.

Field	Value
Name	Type NetWitness-alarm1 .
Type	Real Time
Summary Interval	3600
Event Group	Enter the name of the Event Group on which you want to alert.
Filter	None
Threshold	None
Notification Rules	Select NW-SNMP .

11. Click **OK > Commit**.
12. Click **Enterprise View**, and expand the device nodes.
13. Right-click **Alarm Tool agent**, and select **Associate Alarm Tool Policy**.
14. In the Alarm Tool Policy window, select the Alarm Tool Policy that contains the newly created alarm, and click **OK**.
15. Right-click the Alarm Tool agent, and select **Deploy**.

The SNMPv1 variables are now set, and Dragon starts sending traps to RSA NetWitness Suite.

Configure Dragon version 5.x or 6.x

To set up Dragon 5.x or 6.x:

1. Log on to Dragon IDS as dragon-admin.
2. Click **Alarmtool > Notification Rules > New Notification Rule**.
3. In the Rule Name field, enter a name for the rule, for example, **NW-SNMP**.
4. From the drop-down list, select a time period. RSA recommends selecting **Working Hours**.
5. Click **Save**.

Note: The system adds **SNMPv1** to the notification rule you created.

6. Ensure that the following fields are displayed in the proper format:
 - Transport
 - Port
 - OID
 - Trap Type
 - Specific Type
 - Community

If the following fields are null, click the **x** next to SNMP version 1 to delete SNMPv1, and from Alarmtool wizard, select **SNMPv1**.

7. Enter the correct values for each of the following fields:
 - Transport
 - Server
 - Port
 - OID
 - Trap Type
 - Specific Type

- Community
- Message

8. In the Message field, type the following:

```
%ALERT% %SENSOR% %SIP% %DIP% %SPORT% %DPORT% %PROTO% %DIR%  
%NAME% %DATE% %TIME% %DATA%
```

9. Click **Save**.


The SNMPv1 variables are now set, and Dragon starts sending traps to RSA NetWitness Suite.

Configure RSA NetWitness Suite for SNMP

Add the SNMP Event Source Type

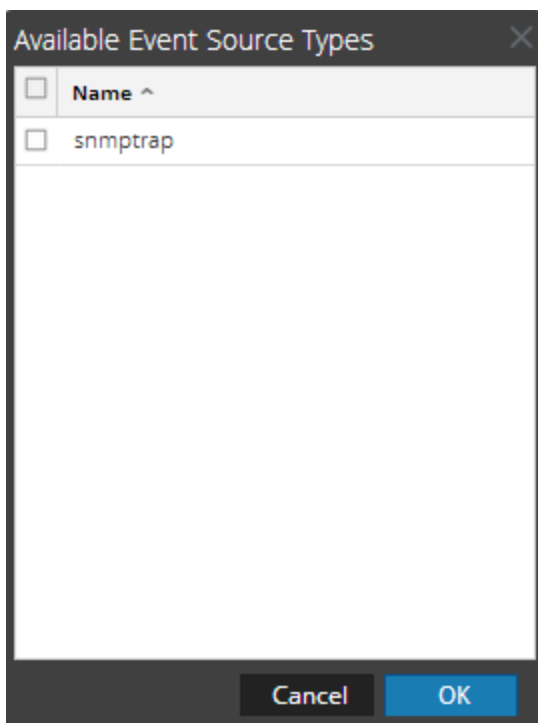
Note: If you have previously added the **snmptrap** type, you cannot add it again. You can edit it, or manage users.

Add the SNMP Event Source Type:

1. In the **RSA NetWitness Suite** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **SNMP/Config** from the drop-down menu.

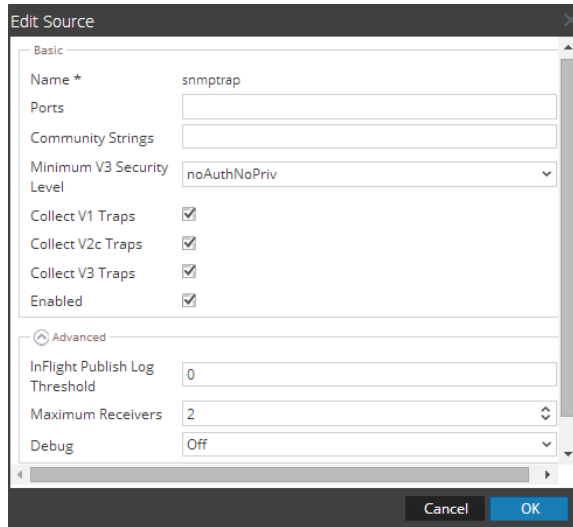
The Sources panel is displayed with the existing sources, if any.

5. Click **+** to open the **Available Event Source Types** dialog.



6. Select **snmptrap** from the Available Event Source Types dialog and click **OK**.

7. Select **snmptrap** in the Event Categories panel.
8. Select **snmptrap** in the Sources panel and then click the Edit icon to edit the parameters.



The screenshot shows the 'Edit Source' dialog box for the 'snmptrap' event source. The dialog is divided into two sections: 'Basic' and 'Advanced'. The 'Basic' section contains the following fields and options:

- Name *: snmptrap
- Ports: [Empty text box]
- Community Strings: [Empty text box]
- Minimum V3 Security Level: noAuthNoPriv (dropdown menu)
- Collect V1 Traps:
- Collect V2c Traps:
- Collect V3 Traps:
- Enabled:

The 'Advanced' section contains the following fields and options:

- InFlight Publish Log Threshold: 0
- Maximum Receivers: 2 (spin box)
- Debug: Off (dropdown menu)


At the bottom of the dialog, there are 'Cancel' and 'OK' buttons.

9. Update any of the parameters that you need to change.

(Optional) Configure SNMP Users

If you are using SNMPv3, follow this procedure to update and maintain the SNMP v3 users.

Configure SNMP v3 Users

1. In the **RSA NetWitness Suite** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **SNMP/SNMP v3 User Manager** from the drop-down menu.

The SNMP v3 User panel is displayed with the existing users, if any.

5. Click **+** to open the **Add SNMP User** dialog.

6. Fill in the dialog with the necessary parameters. The available parameters are described below..

SNMP User Parameters

The following table describes the parameters that you need to enter when you create an SNMP v3 user.

Parameter	Description
Username *	User name (or more accurately in SNMP terminology, security name). RSA NetWitness Suite uses this parameter and the Engine ID parameter to create a user entry in the SNMP engine of the collection service. The Username and Engine ID combination must be unique (for example, logcollector).
Engine ID	(Optional) Engine ID of the event source. For all event sources sending SNMP v3 traps to this collection service, you must add the username and engine id of the sending event source. For all event sources sending SNMPv3 informs, you must add just the username with a blank engine id.
Authentication Type	(Optional) Authentication protocol. Valid values are as follows: <ul style="list-style-type: none"> • None (default) - only security level of noAuthNoPriv can be used for traps sent to this service • SHA - Secure Hash Algorithm

Parameter	Description
	<ul style="list-style-type: none"> • MD5 - Message Digest Algorithm
Authentication Passphrase	Optional if you do not have the Authentication Type set. Authentication passphrase.
Privacy Type	(Optional) Privacy protocol. You can only set this parameter if Authentication Type parameter is set. Valid values are as follows: <ul style="list-style-type: none"> • None (default) • AES - Advanced Encryption Standard • DES - Data Encryption Standard
Privacy Passphrase	Optional if you do not have the Privacy Type set. Privacy passphrase.
Close	Closes the dialog without adding the SNMP v3 user or saving modifications to the parameters.
Save	Adds the SNMP v3 user parameters or saves modifications to the parameters.

Copyright © 2017 EMC Corporation. All Rights Reserved.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.