

JUNIPER NETWORKS STRM TECHNICAL NOTE

CUSTOMIZING SNMP TRAPS

FEBRUARY 2008

In the Custom Rules Wizard, you can configure the Custom Rules Engine to send Simple Network Management Protocol (SNMP) traps as a result of rules configured conditions being met. You can customize the SNMP configuration parameters that appear in the Custom Rules Wizard as well as the SNMP traps that the Custom Rule Engine sends.

This document provides information on customizing SNMP traps including:

- [Customizing the Custom Rules Wizard SNMP Parameters](#)
- [Customizing SNMP Traps](#)
- [Defining Multiple Trap Types](#)



Note: The procedures in this document requires experience with SNMP and manipulating XML files. For more information on SNMP, see Internet Request for Comment (RFC) 1157.

Customizing the Custom Rules Wizard SNMP Parameters

By default, the Custom Rules Wizard allows you to send SNMP traps whenever a rule meets the configured conditions. However, the SNMP trap parameters only appear in the Custom Rules Wizard when SNMP is enabled within the system settings. You can customize the SNMP Trap parameter to enable you to customize the information that is sent as a result of the rules conditions being met.



Note: For more information on the Custom Rules Wizard and STRM system settings, see the STRM Administration Guide.

To customize SNMP parameters that appear in the Custom Rules Wizard:

Step 1 Log in to STRM as root.

Step 2 Open the following file:

```
/opt/qradar/conf/snmp.xml
```

The default file appears. The portion of the file that is necessary for customizing the SNMP parameters in the Custom Rules Wizard is as follows:

```
<snmp>
```

```
<! -- Example Custom Fields -->
<!--
  <creSNMPResponse name='snmp_response_1">
    <custom name="MyColor">
      <string label="What is your favorite color?"/>
    </custom>
    <custom name="MyCategory">
      <list label="Select a category">
        <option label="Label1" value="Category1">
        <option label="Label2" value="Category2"/>
      </list>
    </custom>
  </creSNMPResponse>
```

Step 3 Uncomment the fields.

Step 4 Update the fields, as necessary.

You can configure two types of fields to appear for SNMP traps:

- **Strings** — Enables you to include a text box for the user to enter text.
- **List** — Enables you to include drop-down list boxes so the user can select options.

For example, for the default options in the snmp.xml file, the following would appear in the Custom Rules Wizard.



Note: To include the customized parameters in the SNMP trap, see [Customizing SNMP Traps](#).

Step 5 Save and exit the file.

Customizing SNMP Traps

SNMP allows STRM to send traps, which provides information when rule conditions have been met. By default, STRM adheres to the QRadar MIB. You can customize the output of the SNMP traps to adhere to any MIB you wish.



Note: For more information on the STRM MIB, see *Appendix A of the STRM Administration Guide*.

To customize SNMP traps:

Step 1 Log in to STRM as root.

Step 2 Open the following file:

```
/opt/qradar/conf/snmp.xml
```

The default file appears. The portion of the file that is necessary for customizing SNMP traps is as follows:

```
<!-- Default QRADAR TRAP -->
<creSNMPTrap name="q1CRENotification" OID="1.3.6.1.4.1.20212.200.0" version="3">
  <variableBinding name="q1NotificationData" OID="1.3.6.1.4.1.20212.100">
```

```

<string>
    <value source="NATIVE">DATE_AND_TIME</value>
    <value source="TEXT">QRADAR Custom Rule Engine Notification -
    Rule '</value>
    <value source="NATIVE">RULE_NAME</value>
    <value source="TEXT">' has fired.</value>
    <value source="NATIVE">SOURCE_IP</value>
    <value source="TEXT">:</value>
    <value source="NATIVE">SOURCE_PORT</value>
    <value source="TEXT">-></value>
    <value source="NATIVE">DESTINATION_IP</value>
    <value source="TEXT">:</value>
    <value source="NATIVE">DESTINATION_PORT</value>
    <value source="TEXT"> </value>
    <value source="NATIVE">PROTOCOL</value>
    <value source="TEXT">, Event Name:</value>
    <value source="NATIVE">EVENT_NAME</value>
    <value source="TEXT">, QID:</value>
    <value source="NATIVE">QID</value>
    <value source="TEXT">, Category:</value>
    <value source="NATIVE">CATEGORY</value>
    <value source="TEXT">, Notes:</value>
    <value source="NATIVE">RULE_DESCRIPTION</value>
</string>
</variableBinding>
</creSNMPTrap>
</snmp>

```

Step 3 If you wish to change the trap that is used for SNMP trap notification, update the following line with the appropriate trap OID:

```

<creSNMPTrap name="q1CRENotification"
OID="1.3.6.1.4.1.20212.200.0" version="3">

```

Step 4 If you wish to change the variable binding that is used for SNMP trap notification, update the following line with the appropriate information:

```

<variableBinding name="q1NotificationData"
OID="1.3.6.1.4.1.20212.100">

```

Step 5 Update the variable binding information, as necessary. You can include one of the following values:

- **string** — Enables you to configure multiple values within the variable bindings.

- **integer** — Enables you to include a numerical value in the variable binding. For example:

```
<integer>
<value source="CUSTOM" default="0">MyCategory</value>
</integer>
```

- **oid** — Enables you to include OID information in the variable binding. For example:

```
<oid>
<value source="CUSTOM" default="5.6.7.8.9">MyOID</value>
</oid>
```

- **ipaddress** — Enables you to include IP address information in the variable binding. For example:

```
<ipAddress>
<value source="NATIVE">SOURCE_IP</value>
</ipAddress>
```

For each of the above options, you may include one of the following fields:

- **NATIVE** — Specify a native event from STRM. For the NATIVE value, you can use any of the following fields:
 - SOURCE_IP
 - DESTINATION_IP
 - SOURCE_PORT
 - DESTINATION_PORT
 - PROTOCOL
 - CATEGORY
 - EVENT_NAME
 - QID
 - RULE_NAME
 - RULE_DESCRIPTION
 - LOCALHOST
 - DATE_AND_TIME
- **TEXT** — Specify the text that you wish to include in the SNMP trap.
- **CUSTOM** — Specify the custom SNMP trap information. This is information that you configured in [Customizing the Custom Rules Wizard SNMP Parameters](#). For example, if you used the default file information and wished to include this information in the SNMP Trap, you should include the following:


```
<value source="CUSTOM" default="blue">MyColour</value>
```

For example, if you use the default information, the following SNMP trap appears, if the rule conditions are met:

```
2006-07-11 16:06:44 NET-SNMP version 5.2.1 Started.
```

```
Cold Start: INFORM, SNMP v3, user admin, context
```

```
-SNMPv2-MIB::sysUptime.0 - Timeticks: (555) 0:00:05.55
```

```
-SNMPv2-MIB::snmpTrapOID.0 = OID:
```

```
SNMPv2-SMI::enterprise.20212.200.0
```

```
-SNMPv2-SMI::enterprises.20212.100 = STRING: "Tue Jul 11
```

```
16:06:55 ADT 2006 QRADAR Custom Rule Engine Notification - Rule
'Network Scan' has fired. 172.168.1.42:32000 -> 10.100.100.25:80
6, Event Name: EmptyEventName, QID: 42, Category: 1004, Notes: A
scan of the network was detected"
```

Step 6 Save and exit the file.

Defining Multiple Trap Types

STRM allows you to define multiple trap types. When there is more than one type defined, the Custom Rules Wizard allows you to select from the available types for each rule response.

To create additional trap types:

Step 1 Log in to STRM as root.

Step 2 Go to the following directory:

```
/opt/qradar/conf
```

Step 3 Copy the snmp.xml file to a new file with the .xml extension. For example:

```
cp snmp.xml <filename>.xml
```

Step 4 If necessary, edit the new file according to the instructions in [Customizing SNMP Traps](#).

Step 5 Open the following file:

```
snmp-master.xml
```

Step 6 Find the following line:

```
<include name="q1Notification" uri="snmp.xml"/>
```

Step 7 Select that line and copy/paste it below the selected line.

Step 8 In the new line:

a Change the `name` variable to a chosen name.

b Change the `uri` variable to the file name specified in [Step 3](#).

For example:

```
<include name="q1Notification" uri="snmp.xml"/>
<include name="filename" uri="filename.xml"/>
```

Step 9 Save and close the file.

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA

Copyright © 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Part Number 530-xxxxxx-01