



**Security Threat Response Manager**

## **Managing Sensor Devices**

***Release 2008.1***

**Juniper Networks, Inc.**

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

**[www.juniper.net](http://www.juniper.net)**

Part Number: 530-023504-01, Revision 1

## Copyright Notice

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.

## FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense. The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Reorient or relocate the receiving antenna. Increase the separation between the equipment and receiver. Consult the dealer or an experienced radio/TV technician for help. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

## Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

*Managing Sensor Devices*  
Release 2008.1

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

31 January 2008—Revision 1

The information in this document is current as of the date listed in the revision history.

# CONTENTS

---

## 1 MANAGING SENSOR DEVICES

Configuring STRM to Receive Events	3
Managing Sensor Devices	4
Adding a Sensor Device	4
Editing Sensor Devices	6
Enabling/Disabling Sensor Devices	7
Deleting a Sensor Device	8
Configuring Protocols	8
Adding a Protocol	8
Editing a Protocol	15
Deleting a Protocol	16
Grouping Sensor Devices	16
Viewing Sensor Devices Using Groups	16
Creating a Group	17
Editing a Group	18
Copying a Sensor Device to Another Group	18
Deleting a Sensor From a Group	19

---

## 2 SUPPORTED DSMS



# ABOUT THIS GUIDE

This preface provides the following guidelines for using the *Managing Sensor Devices Guide*:

- [Documentation Feedback](#)
- [Requesting Support](#)

---

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. Send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <http://www.juniper.net/techpubs/docbug/docbugreport.html>. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version

---

## Requesting Support

Open a support case using the Case Management link at <http://www.juniper.net/support/> or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).



# 1

## MANAGING SENSOR DEVICES

You can configure STRM to log and correlate events received from external sources such as security equipment (for example, firewalls and IDSs) and network equipment (for example, switches and routers). Sensor devices allow you to integrate STRM with these external devices. This chapter provides information on configuring sensor devices to the system including:

- [Configuring STRM to Receive Events](#)
- [Managing Sensor Devices](#)
- [Configuring Protocols](#)
- [Grouping Sensor Devices](#)

---

### Configuring STRM to Receive Events

STRM allows you to automatically discover sensor devices in your deployment that are sending syslog messages. Any sensor devices that are automatically discovered by STRM appear in the Sensor Devices window. Automatic discovery of sensor devices can be configured on a per Event Collector basis using the Auto Detection Enabled parameter in the Event Collector configuration. For more information, see the *STRM Administration Guide*, Using the Deployment Editor.

To configure STRM to receive events from devices, you must:

- Step 1** Configure the device to send events to STRM. See [Chapter 2 Supported DSMs](#). For information on configuring DSMs, see the *Configuring DSMs Guide* and your vendor documentation.
- Step 2** Configure STRM to receive events from specific devices. See [Managing Sensor Devices](#).



**Note:** You must have administrative privileges to configure sensor devices in STRM. For more information on accessing the Administration Console, see the *STRM Administration Guide*.

- Step 3** Configure the necessary protocols. See [Configuring Protocols](#).

**Managing Sensor Devices**

A sensor device provides events to your deployment through DSMs. Using Administration Console, you can:

- Add a sensor device. See [Adding a Sensor Device](#).
- Edit an existing sensor device. See [Editing Sensor Devices](#).
- Enable or disable a sensor device. See [Enabling/Disabling Sensor Devices](#).
- Delete a sensor device. See [Deleting a Sensor Device](#).

**Adding a Sensor Device**

To add a sensor device to your deployment:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **Sensor Devices** icon.  
The Sensor Devices window appears.

Name	Group	Device Type	Enabled	Hostname/IP	Configuration	Target Event Collector	Credibility	Autodiscovered
Auto-discovered LinuxServer at qafedora		Linux login messages	true	qafedora	Syslog :: default syslog	eventcollector0 :: vanquish	5	true
Auto-discovered Pix at apophis		Cisco PIX Firewall	true	apophis	Syslog :: default syslog	eventcollector0 :: vanquish	5	true
Auto-discovered Snort at wolverine		Snort Open Source IDS	true	wolverine	Syslog :: default syslog	eventcollector0 :: vanquish	5	true

Displaying 1 to 3 of 3 items

- Step 3** Click **Add**.  
The Add a sensor device window appears.

**Add a sensor device**

Device Name:

Sensor Device Type: 3Com 8800 Series Switch

Protocol Configuration: Syslog :: default syslog

Device Description:

Device Hostname/IP:

Credibility: 5

Target Event Collector: eventcollector0 :: vanquish

Coalescing Events: Yes

Store Event Payload: Yes

Save Cancel

- Step 4** Enter values for the parameters:

**Table 1-1** Adding a Sensor Device Parameters

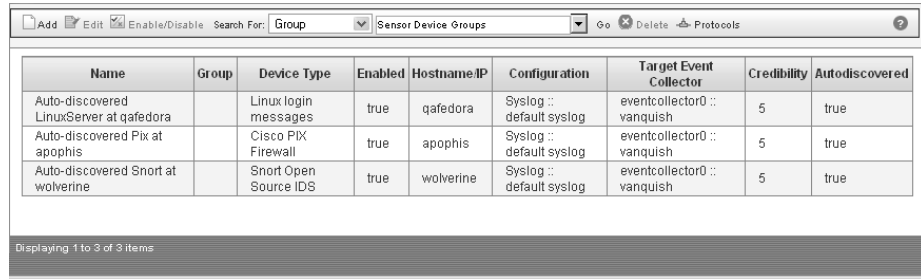
Parameter	Description
Device Name	Specify the desired name of the device.
Sensor Device Type	Using the drop-down list, select the type of sensor device you wish to add.
Protocol Configuration	Using the drop-down list box, select the protocol you wish to use for this sensor device. If the device uses syslog, a default syslog configuration is automatically applied. For more information on configuring protocols, see <a href="#">Adding a Protocol</a> .
Device Description	Specify a description for the sensor device (optional).
Device Hostname/IP	Specify the hostname or IP address for the device. If you wish to add the device using the hostname, please note that you must enter the hostname as it exactly appears in the logs sent to STRM. Otherwise, STRM will not process the events.
Credibility	Specify the credibility of the device. The range is from 0 to 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Using the drop-down list box, select the Event Collector you wish to use as the target for this device.
Coalescing Events	Enables or disables the ability of a sensor device to coalesce (bundle) events. The default is Yes.  By default, all auto detected sensor devices use the value configured in the Coalescing Events parameter in the System Setting window. However, when you create a new sensor device or update the configuration for an auto detected sensor device, the value configured in the individual sensor device is the value used by the sensor device. For more information, see the <i>STRM Administration Guide</i> .
Store Event Payload	Enables or disables the ability for a sensor device to store event payload information. The default is Yes.  By default, all auto detected sensor devices use the value configured in the Store Event Payload parameter in the System Setting window. However, when you create a new sensor device or update the configuration for an auto detected sensor device, the value configured in the individual sensor device is the value used by the sensor device. For more information, see the <i>STRM Administration Guide</i> .

**Step 5** Click **Save**.

The Sensor Devices window appears.

**Editing Sensor Devices** To edit a sensor device:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **Sensor Devices** icon.  
The Sensor Devices window appears.



- Step 3** Select the sensor device you wish to edit.
- Step 4** Click **Edit**.  
The Edit a sensor device window appears.



- Step 5** Edit values for the parameters, as necessary:

**Table 1-2** Editing a Sensor Device Parameters

Parameter	Description
Device Name	Specify the desired name of the device.
Protocol Configuration	Using the drop-down list box, select the protocol you wish to use for this sensor device. If the device uses syslog, a default syslog configuration is automatically applied. For more information on configuring protocols, see <a href="#">Adding a Protocol</a> .
Device Description	Specify a description for the sensor device (optional).
Device Hostname/IP	Specify the hostname or IP address for the device.

**Table 1-2** Editing a Sensor Device Parameters (continued)

Parameter	Description
Credibility	Specify the credibility of the device. The range is from 0 to 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from source devices. Credibility increases as the multiple sources report the same event. The default is 5.
Target Event Collector	Using the drop-down list box, select the Event Collector you wish to use as the target for this device.
Coalescing Events	<p>Enables or disables the ability of a sensor device to coalesce (bundle) events. The default is Yes.</p> <p>By default, all auto detected sensor devices use the value configured in the Coalescing Events parameter in the System Setting window. However, when you create a new sensor device or update the configuration for an auto detected sensor device, the value configured in the individual sensor device is the value used by the sensor device. For more information, see the <i>STRM Administration Guide</i>.</p>
Store Event Payload	<p>Enables or disables the ability for a sensor device to store event payload information. The default is Yes.</p> <p>By default, all auto detected sensor devices use the value configured in the Store Event Payload parameter in the System Setting window. However, when you create a new sensor device or update the configuration for an auto detected sensor device, the value configured in the individual sensor device is the value used by the sensor device. For more information, see the <i>STRM Administration Guide</i>.</p>

**Step 6** Click **Save**.

The Sensor Devices window appears.

**Enabling/Disabling Sensor Devices** To enable or disable sensor devices:

**Step 1** In the Administration Console, click the **SIM Configuration** tab.

The SIM Configuration panel appears.

**Step 2** Click the **Sensor Devices** icon.

The Sensor Devices window appears.

Name	Group	Device Type	Enabled	Hostname/IP	Configuration	Target Event Collector	Credibility	Autodiscovered
Auto-discovered LinuxServer at qafedora		Linux login messages	true	qafedora	Syslog :: default syslog	eventcollector0 :: vanquish	5	true
Auto-discovered Pix at apophis		Cisco PIX Firewall	true	apophis	Syslog :: default syslog	eventcollector0 :: vanquish	5	true
Auto-discovered Snort at wolverine		Snort Open Source IDS	true	wolverine	Syslog :: default syslog	eventcollector0 :: vanquish	5	true

Displaying 1 to 3 of 3 items

**Step 3** Select the sensor device you wish to enable or disable.

**Step 4** Click **Enable/Disable**.

When a sensor device is enabled, the Enabled column indicates true. When a sensor device is disabled, the Enabled column indicates false.



**Note:** If you are unable to enable a sensor device, you may have exceeded your license restrictions. Consult your licensing agreement for more information.

**Deleting a Sensor Device**

To delete a sensor device:

- Step 1** In the Administration Console, click the **SIM Configuration** tab. The SIM Configuration panel appears.
- Step 2** Click the **Sensor Devices** icon. The Sensor Devices window appears.
- Step 3** Select the sensor device you wish to delete.
- Step 4** Click **Delete**.
- Step 5** A confirmation window appears.
- Step 6** Click **OK**.

**Configuring Protocols**

You can configure protocols for your sensor devices using the Administration Console in the SIM Configuration tab or the Sensor Devices window. The below procedure provides information on configuring protocols using the Manage Protocol Configurations icon in the SIM Configuration interface.

Using the Administration Console, you can:

- Add a protocol. See [Adding a Protocol](#).
- Edit a protocol. See [Editing a Protocol](#).
- Delete a protocol. See [Deleting a Protocol](#).

**Adding a Protocol**

To add a protocol:

- Step 1** In the Administration Console, click the **SIM Configuration** tab. The SIM Configuration panel appears.

**Step 2** Click the **Protocol Configuration** icon.

The Sensor Device Protocol Configurations window appears.



**Step 3** Click **Add**.

The Add a protocol configuration window appears.

**Step 4** Enter values for the parameters:

- **Configuration Name** - Specify a name you wish to assign to this protocol configuration.
- **Protocol** - Using the drop-down list box, select the protocol you wish to use for this protocol configuration. See [Step 5](#).

**Step 5** Choose one of the following:

- a If you select JDBC, go to [Step 6](#).
- b If you select JDBC:SiteProtector, go to [Step 7](#).
- c If you select JuniperNSM, go to [Step 8](#).
- d If you select LEA, go to [Step 9](#).
- e If you select SNMP, go to [Step 11](#).
- f If you select SDEE, go to [Step 10](#).

**Step 6** If you have selected JDBC:

- a Click **Configure**.

The JDBC Configuration window appears.

b Enter values for the parameters:

- **Database Type** - Using the drop-down list box, select the type of database that you wish to use for the event source. The options include Microsoft MSDE, Postgres, MySQL, and Oracle.
- **Database Name** - Specify the name of the database you wish to connect.
- **Table Name** - Specify the name of the table or view that includes the event records.
- **Select List** - Specify the list of fields that you wish to include in the events. You can use a comma separated list or specify \* for all fields from the table or view.
- **Compare Field** - Specify a numeric value or timestamp field that you wish to use to identify new events added between queries to the table.
- **Hostname** - Specify the IP address or hostname of the database server.
- **Port** - Specify the port number used by the database server. The default is 1433.
- **Username** - Specify the database username.
- **Password** - Specify the database password.
- **Polling Interval** - Specify the polling interval, which is the number of seconds between queries to the event table. The default is 10.

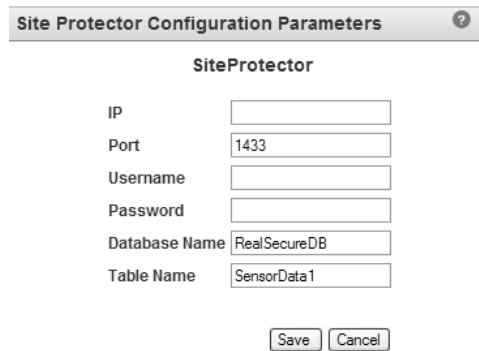
c Click **Save**.

The Protocol Configurations window appears.

**Step 7** If you have selected JDBC:SiteProtector:

a Click **Configure**.

The configuration window appears.



The dialog box is titled "Site Protector Configuration Parameters" and contains the following fields:

SiteProtector	
IP	<input type="text"/>
Port	<input type="text" value="1433"/>
Username	<input type="text"/>
Password	<input type="text"/>
Database Name	<input type="text" value="RealSecureDB"/>
Table Name	<input type="text" value="SensorData1"/>

At the bottom of the dialog are "Save" and "Cancel" buttons.

b Enter values for the parameters:

- **IP** - Specify the IP address for the ISS SiteProtector device.
- **Port** - Specify the port used by the server database to listen for remote connections. The default port is 1433.
- **Username** - Specify the user name. This username must match the value entered when defining the database user when configuring ISS SiteProtector. For more information, see the *Configuring DSM Guide*.
- **Password** - Specify the user password. This password must match the value entered when defining the database user when configuring the ISS SiteProtector. For more information, see the *Configuring DSM Guide*.
- **Database Name** - Specify the database name for the ISS SiteProtector. Default name is RealSecure DB.
- **Table Name** - Specify the table name used to store the events. Default name is SensorData1.

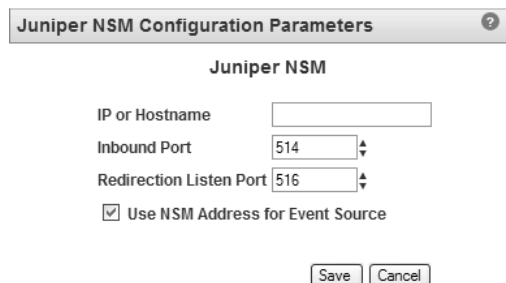
c Click **Save**.

The Protocol Configurations window appears.

**Step 8** If you selected JuniperNSM:

a Click **Configure**.

The Juniper NSM Configuration Parameters window appears.



The dialog box is titled "Juniper NSM Configuration Parameters" and contains the following fields:

Juniper NSM	
IP or Hostname	<input type="text"/>
Inbound Port	<input type="text" value="514"/>
Redirection Listen Port	<input type="text" value="516"/>
<input checked="" type="checkbox"/> Use NSM Address for Event Source	

At the bottom of the dialog are "Save" and "Cancel" buttons.

b Enter values for the parameters:

- **IP or Hostname** - Specify the IP address or hostname of the Juniper NSM server.

- **Inbound Port** - Specify the port to which the Juniper NSM sends communications.
- **Redirection Listen Port** - Specifies the port to which traffic is forwarded.
- **Use NSM Address for Event Source** - Select the check box if you wish to use the Juniper NSM server's IP address instead of the managed device's IP address for an event source. If you do not wish to use the Juniper NSM server's address, you must create a separate sensor device for each device managed by the NSM.

c Click **Save**.

The Protocol Configurations window appears.

**Step 9** If you selected LEA:

a Click **Configure**.

The LEA Configuration Parameters window appears.

b Enter values for the parameters:

- **Server IP or Hostname** - Specify the IP address or hostname of the server.
- **Server Port** - Specify the port used for OPSEC communication. The default is 18184.
- **User Server IP for Event Source** - Select the check box if you wish to use the LEA server's IP address instead of the managed device's IP address for an event source. If you do not wish to use the LEA server's IP address, you must create a separate sensor device for each device managed by the LEA server.
- **Authentication Type** - Using the drop-down list box, select the authentication type you wish to use for this LEA configuration. The options are sslca, sslca\_clear, or clear.

- **SIC Name** - This option only appears if SSL Certificate Authority (sslca) or sslca\_clear is selected as the authentication type. Specify the Secure Internal Communications (SIC) name of the OPSEC Application Object. The SIC name is the distinguished name (DN) of the application.
- **Entity SIC Name** - This option only appears if SSL Certificate Authority (sslca) or sslca\_clear is selected as the authentication type. Specify the SIC name of the server.
- **Specify Certificate** - This option only appears if SSL Certificate Authority (sslca) or sslca\_clear is selected as the authentication type. Select the check box if you wish to specify a certificate for this LEA configuration. If you select the check box, the following parameter appears. STRM attempts to pull the certificate using these parameters when the certificate is required:

**Certificate Filename** - Specify the certificate you wish to use for this configuration.

If you clear the Specify Certificate check box, the following parameters appear:

**Certificate Authority IP or Hostname** - Specify the IP address or hostname of the SmartCenter server from which you wish to pull your certificate.

**Pull Certificate Password** - Specify the password you wish to use when requesting a certificate.

**OPSEC Application** - Specify the name of the application you wish to use when requesting a certificate.

- c Click **Save**.

The Protocol Configurations window appears.

**Step 10** If you have selected SDEE:

- a Click **Configure**.

The SDEE Configuration Parameters window appears.

**SDEE Configuration Parameters** ?

**SDEE**

URL

Username

Password

Max Events per Query

Severity Filter Low

Severity Filter Medium

Severity Filter High

Force Subscription

- b Enter values for the following parameters:

- **URL** - Specify the URL required to access the device, for example, `https://www.mysdeeserver.com/cgi-bin/sdee-server`. You must use an http or https URL.

If you are using RDEP (for Cisco IDS v4.0), the URL should have `/cgi-bin/event-server` at the end. For example:

`https://www.my-rdep-server.com/cgi-bin/event-server`

If you are using SDEE/CIDEE (for Cisco IDS v5.x), the URL should have `/cgi-bin/sdee-server` at the end. For example:

`https://www.my-sdee-server/cgi-bin/sdee-server`

- **Username** - Specify the user name. This username must match the SDEE URL username used to access the SDEE URL.
  - **Password** - Specify the user password. This password must match the SDEE URL password used to access the SDEE URL.
  - **Max Events Per Query** - Specify the maximum number of events to retrieve per query. The default is 100.
  - **Severity Filter** - Select the check boxes you wish to use to configure the severity level. A sensor devices that supports SDEE returns only the events that match this severity level. Options include: Low, Medium, and High. By default, all check boxes are selected. You must have at least one check box selected.
  - **Force Subscription** - Select the check box if you wish to enforce this connection. Select yes to force the server to drop it's least active connection to accept this connection; select no if you wish to not force this connection. By default, the check box is selected.
- c Click **Save**.
- The Protocol Configurations window appears.

**Step 11** If you have selected SNMPv2:

- a Click **Configure**.
- The SNMPv2 Configuration Parameters window appears.

- b In the Community field, specify the SNMP community, such as public. This parameter only applies if you are using SNMPv2c. The default is Public.
- c Click **Save**.
- The Protocol Configurations window appears.

**Step 12** If you have selected SNMPv3:

a Click **Configure**.

The SNMP Configuration Parameters window appears.

b Enter values for the parameters:

- **Authentication Protocol** - Using the drop-down list box, select the algorithm you wish to use to authenticate SNMP traps. This parameter is required if you are using SNMPv3. The default is MD5.
- **Authentication Password** - Specify the password you wish to use to authenticate SNMP. This parameter is required if you are using SNMPv3.
- **Decryption Protocol** - Using the drop-down list box, select the protocol you wish to use to decrypt SNMP traps. This parameter is required if you are using SNMPv3. The default is AES256.
- **Decryption Password** - Specify the password used to decrypt SNMP traps. This parameter is required if you are using SNMPv3.
- **User** - Specify the user access for this protocol. The default is AdminUser.

c Click **Save**.

The Protocol Configurations window appears.

**Editing a Protocol** To edit an existing protocol:

**Step 1** In the Administration Console, click the **SIM Configuration** tab.

The SIM Configuration panel appears.

**Step 2** Click the **Protocol Configuration** icon.

The Protocol Configurations window appears.

**Step 3** Select the protocol you wish to edit.

**Step 4** Click **Edit**.

The configuration parameters for the selected protocol appears.

**Step 5** Update parameters, as necessary. For more information on protocol configuration, see [Adding a Protocol](#).

**Step 6** Click **Save**.

The Protocol Configurations window appears.

**Deleting a Protocol** To delete a protocol:



**Note:** When you delete a protocol that is currently being used by a sensor device, the sensor device is disabled.

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **Protocol Configuration** icon.  
The Protocol Configurations window appears.
- Step 3** Select the protocol you wish to delete.
- Step 4** Click **Delete**.  
A confirmation window appears.
- Step 5** Click **Ok**.

## Grouping Sensor Devices

You can view sensor devices based on functionality. Categorizing your sensor devices into groups allows you to efficiently view and track your devices. For example, you can view all devices by name. By default, the sensor devices interface displays all sensor devices.



**Note:** You must have administrative access to create, edit, or delete groups. For more information on user roles, see the *STRM Administration Guide*.

This sections provides information on grouping reports including:

- [Viewing Sensor Devices Using Groups](#)
- [Creating a Group](#)
- [Editing a Group](#)
- [Copying a Sensor Device to Another Group](#)
- [Deleting a Sensor From a Group](#)

## Viewing Sensor Devices Using Groups

To view sensor devices using groups:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **Sensor Devices** icon.  
The Sensor Devices window appears.
- Step 3** From the Search For drop-down list box, select the group option you wish to display.
- Step 4** In the field next to the drop-down list box, specify the specific group criteria you wish to view.
- Step 5** Click **Go**.

The group results appear.

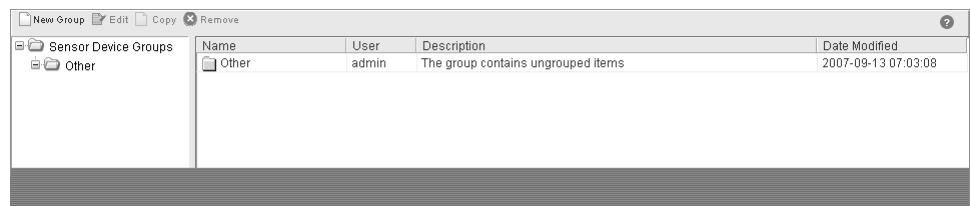
**Creating a Group** To create a group:

**Step 1** In the Administration Console, click the **SIM Configuration** tab.

The SIM Configuration panel appears.

**Step 2** Click the **Sensor Device Groups** icon.

The Sensor Device Groups window appears.



**Step 3** From the menu tree, select the group under which you wish to create a new group.



**Note:** Once you create the group, you can drag and drop menu tree items to change the organization of the tree items.

**Step 4** Click **New Group**.

The Group Properties window appears.

**Group Properties**

Parent: Sensor Device Groups

Name:

Description:

OK Cancel

**Step 5** Enter values for the parameters:

- **Name** - Specify the name you wish to assign to the new group. The name may be up to 255 characters in length.
- **Description** - Specify a description you wish to assign to this group. The description may be up to 255 characters in length.

**Step 6** Click **Ok**.

**Step 7** If you wish to change the location of the new group, click the new group and drag the folder to the desired location in your menu tree.

**Step 8** Close the Groups window.

**Editing a Group** To edit a group:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **Sensor Device Groups** icon.  
The Sensor Device Groups window appears.
- Step 3** From the menu tree, select the group you wish to edit.
- Step 4** Click **Edit**.  
The Group Properties window appears.
- Step 5** Update values for the parameters, as necessary:
  - **Name** - Specify the name you wish to assign to the new group. The name may be up to 255 characters in length.
  - **Description** - Specify a description you wish to assign to this group. The description may be up to 255 characters in length.
- Step 6** Click **Ok**.
- Step 7** If you wish to change the location of the group, click the new group and drag the folder to the desired location in your menu tree.
- Step 8** Close the Groups window.

**Copying a Sensor Device to Another Group** Using the groups functionality, you can copy a sensor device to one or many other groups. To copy a sensor device:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **Sensor Device Groups** icon.  
The Sensor Device Groups window appears.
- Step 3** From the menu tree, select the sensor device you wish to copy to another group.
- Step 4** Click **Copy**.  
The Choose Group window appears.



- Step 5** Select the group(s) to which you wish to copy the sensor device.
- Step 6** Click **Assign Groups**.

**Step 7** Close the Groups window.

**Deleting a Sensor From a Group** To delete a sensor device from a group:



**Note:** Removing a sensor device from a group removes the sensor device from the group. Removing a sensor device does not delete the device from STRM.

**Step 1** In the Administration Console, click the **SIM Configuration** tab.

The SIM Configuration panel appears.

**Step 2** Click the **Sensor Device Groups** icon.

The Sensor Device Groups window appears.

**Step 3** From the menu tree, select the top level group.

**Step 4** From the list of groups, select the item you wish to delete.

**Step 5** Click **Remove**.

A confirmation window appears.

**Step 6** Click **Ok**.

**Step 7** Close the Groups window.



# 2

## SUPPORTED DSMs

Table 2-1 provides information on the DSMs STRM supports.



**Note:** For the latest DSM information and documentation, please see the Qmmunity web site.

**Table 2-1** Supported DSMs

Manufacturer	DSM	Versions Supported	Events Accepted	STRM Recorded Events	Option in STRM	For More Information
3Com	8800 Series Switch	v3.01.30	Syslog	All relevant status and network condition	3Com 8800 Series Switch	www.3com.com
Ambiron	TrustWave ipAngel	v4.0	Syslog	Snort-based events	Ambiron TrustWave ipAngel Intrusion Prevention System (IPS)	www.atwcorp.com
Apache	HTTP Server	v1.3 and above	Syslog	HTTP status	Open Source Apache Webserver	www.apache.org
Apple	Mac OS	X (10)	Syslog	All relevant firewall, web server (access/error), privilege, and information events	Mac OSx	www.apple.com
Array Network	SSL VPN	ArraySP v7.3	Syslog	All relevant events	Array Networks SSL VPN Access Gateway	www.array networks.net
Blue Coat	SG	v4.x and above	Syslog	All relevant events	Blue Coat SG Appliance	www.bluecoat.com
Check Point	FireWall-1	NG, FP1, FP2, FP3, AI R54, AI R55, NGX	Syslog	All relevant events	Check Point Firewall-1	www.checkpoint.com

**Table 2-1** Supported DSMs (continued)

<b>Manufacturer</b>	<b>DSM</b>	<b>Versions Supported</b>	<b>Events Accepted</b>	<b>STRM Recorded Events</b>	<b>Option in STRM</b>	<b>For More Information</b>
	VPN-1	NG, FP1, FP2, FP3, AI R54, AI R55, NGX	Syslog	All relevant events	Check Point Firewall-1	<a href="http://www.checkpoint.com">www.checkpoint.com</a>
	Provider-1	NG, FP1, FP2, FP3, AI R54, AI R55, NGX	Syslog	All relevant events	Check Point Firewall-1	<a href="http://www.checkpoint.com">www.checkpoint.com</a>
	OPSEC using Leapipe	NG, FP1, FP2, FP3, AI R54, AI R55, NGX	OPSEC	All relevant events	Check Point Firewall-1	<a href="http://www.checkpoint.com">www.checkpoint.com</a>
Cisco	ACS	v4.1 and above if directly from ACS  v3.x and above if using ALE	Syslog	All relevant events	Cisco ACS	<a href="http://www.cisco.com/public/support/tac/documentation.html">www.cisco.com/public/support/tac/documentation.html</a>
	ASA	v7.x and above	Syslog	All relevant events	Cisco Adaptive Security Appliance (ASA)	<a href="http://www.cisco.com/public/support/tac/documentation.html">www.cisco.com/public/support/tac/documentation.html</a>
	CatOS for catalyst systems	v7.3 and above	Syslog	All relevant events	Cisco CatOS for Catalyst Switches	<a href="http://www.cisco.com/public/support/tac/documentation.html">www.cisco.com/public/support/tac/documentation.html</a>
	IDS/IPS	v5.x and v6.x	SDEE	All relevant events	Cisco Intrusion Prevention System (IPS)	<a href="http://www.cisco.com/public/support/tac/documentation.html">www.cisco.com/public/support/tac/documentation.html</a>
	Firewall Service Module (FWSM)	v2.1 and above	Syslog	All relevant events	Cisco Firewall Services Module (FWSM)	<a href="http://www.cisco.com/public/support/tac/documentation.html">www.cisco.com/public/support/tac/documentation.html</a>
	Catalyst Switch	IOS, 12.2, 12.5, and above	Syslog	All relevant events	Cisco IOS	<a href="http://www.cisco.com/public/support/tac/documentation.html">www.cisco.com/public/support/tac/documentation.html</a>
	NAC Appliance	v4.x and above	Syslog	All relevant audit, error, failure, quarantine, and infected events	Cisco NAC	<a href="http://www.cisco.com/public/support/tac/documentation.html">www.cisco.com/public/support/tac/documentation.html</a>

**Table 2-1** Supported DSMs (continued)

<b>Manufacturer</b>	<b>DSM</b>	<b>Versions Supported</b>	<b>Events Accepted</b>	<b>STRM Recorded Events</b>	<b>Option in STRM</b>	<b>For More Information</b>
	PIX Firewall	v5.x, v6.3, and above	Syslog	All relevant Cisco PIX events	Cisco PIX Firewall	<a href="http://www.cisco.com/public/support/tac/documentation.html">www.cisco.com/public/support/tac/documentation.html</a>
	IOS	IOS, 12.2, 12.5, and above	Syslog	All relevant events	Depending on your system, choose one of the following: Cisco IOS Cisco 1200 Series Cisco 6500 Series Router Cisco Carrier Routing System Cisco Integrated Services Router	<a href="http://www.cisco.com/public/support/tac/documentation.html">www.cisco.com/public/support/tac/documentation.html</a>
	VPN 3000 Concentrator	VPN 3005, 4.1.7.H	Syslog	All relevant events	Cisco VPN 3000 Series Concentrator	<a href="http://www.cisco.com/public/support/tac/documentation.html">www.cisco.com/public/support/tac/documentation.html</a>
	Security Agent	v4.x and 5.x	SNMP	All relevant events	Cisco Security Agent (CSA)	<a href="http://www.cisco.com/public/support/tac/documentation.html">www.cisco.com/public/support/tac/documentation.html</a>
CyberGuard	Firewall/VPN	KS1000 v5.1	Syslog	All relevant CyberGuard events	CyberGuard TSP Firewall/VPN	<a href="http://www.cyberguard.com/">www.cyberguard.com/</a>
Enterasys	Dragon	v5.0, 6.x, v7.1, v7.2	Syslog and SNMP	All relevant Enterasys Dragon events.	Enterasys Dragon Network IPS	<a href="http://www.enterasys.com">www.enterasys.com</a>
	Matrix Router	v3.5	Syslog and SNMP	SNMP and syslog login, logout, and login failed events	Enterasys Matrix E1 Switch	<a href="http://www.enterasys.com">www.enterasys.com</a>
	Matrix N-Series	v6.x, v7.x	Syslog	All relevant Matrix N3, N5, N7, and N standalone device events	Enterasys N Series Switch	<a href="http://www.enterasys.com">www.enterasys.com</a>

**Table 2-1** Supported DSMs (continued)

<b>Manufacturer</b>	<b>DSM</b>	<b>Versions Supported</b>	<b>Events Accepted</b>	<b>STRM Recorded Events</b>	<b>Option in STRM</b>	<b>For More Information</b>
Extreme Networks	Extreme Ware	v7.7	Syslog	All relevant events	Extreme Networks ExtremeWare Operating System (OS)	www.extreme-networks.com\
F5 Networks	BigIP	v4.5, v9.x	Syslog	All relevant events	F5 Networks BigIP	www.f5.com
ForeScout	CounterACT	v6	Syslog	All relevant events	Forescout CounterACT	www.forescout.com
Fortinet	FortiGate	FortiOS v2.5 and above	Syslog	All relevant events	Fortinet FortiGate Secure Gateway	www.fortinet.com
Universal	Syslog and SNMP		Syslog, SNMP, or SDEE	All relevant events	Universal DSM	
	Authentication Server		Syslog	All relevant events	Configurable Authentication message filter	
	Firewall		Syslog	All relevant events	Configurable Firewall Filter	
IBM	AIX 5L	5.x	Syslog	All relevant events	IBM AIX Server	www.ibm.com
	ISS Proventia	M10 v2.1_2004.1122_15.13.53	SNMP	All relevant events	IBM Proventia Management	www.iss.net
	ISS SiteProtector	v2.0		All relevant events	IBM SiteProtector	www.iss.net
Juniper Network	Secure Access RA	v5.2	Syslog	All relevant events	Juniper Networks Secure Access (SA) SSL VPN	www.juniper.net
	DX		Syslog	All relevant status and network condition events	Juniper DX Application Acceleration Platform	www.juniper.net
	Infranet Controller	UAC v2.0	Syslog	All relevant events	Juniper Networks Infranet Controller	www.juniper.net
	NetScreen Firewall	v5.0 to v5.4	Syslog	All relevant NetScreen Firewall events	Juniper Networks NetScreen Firewall	www.juniper.net

**Table 2-1** Supported DSMs (continued)

<b>Manufacturer</b>	<b>DSM</b>	<b>Versions Supported</b>	<b>Events Accepted</b>	<b>STRM Recorded Events</b>	<b>Option in STRM</b>	<b>For More Information</b>
	NetScreen IDP	v4.0	Syslog	All relevant NetScreen IDP events	Juniper Networks Intrusion Detection and Prevention (IDP)	<a href="http://www.juniper.net">www.juniper.net</a>
	NetScreen NSM	v1.6	Syslog	All relevant NetScreen NSM events	Juniper Networks NetScreen-Security Manager (NSM)	<a href="http://www.juniper.net">www.juniper.net</a>
	Router	v7.0 to v8.5	Syslog	All relevant events	Juniper Networks Routing Platform, Juniper M-Series Multiservice Edge Routing, Juniper MX-Series Ethernet Services Router, or Juniper T-Series Core Platform	<a href="http://www.juniper.net">www.juniper.net</a>
	Steel Belted Radius	v5.x and above	Syslog	All relevant events	Juniper Steel Belted Radius	<a href="http://www.juniper.net">www.juniper.net</a>
Linux	Open Source Linux Login/ Logout Log Red Hat Login/ Logout	v2.4 and above	Syslog	All relevant login, logoff, session opened, session closed, and accepted/failed password events	Linux login messages	
	DHCP Server	v2.4 and above	Syslog	All relevant events from a DHCP server	Linux DHCP Server	
	IPtables kernel	v2.4 and above	Syslog	All relevant Accept, Drop, or Reject events	Linux iptables Firewall	
McAfee	Intrushield	v2.1.x and above	Syslog	All relevant events	McAfee IntruShield Network IPS Appliance	<a href="http://www.mcafee.com">www.mcafee.com</a>
	ePolicy Orchestrator	v 3.0	SNMP	All relevant AntiVirus events	McAfee ePolicy Orchestrator	<a href="http://www.mcafee.com">www.mcafee.com</a>

**Table 2-1** Supported DSMs (continued)

<b>Manufacturer</b>	<b>DSM</b>	<b>Versions Supported</b>	<b>Events Accepted</b>	<b>STRM Recorded Events</b>	<b>Option in STRM</b>	<b>For More Information</b>
MetaInfo	MetalP	v5.7.00-6059 and above	Syslog	All relevant events	MetaInfo MetalP	<a href="http://www.metainfo.com">www.metainfo.com</a>
Microsoft	IIS	v5.x and v6.x	Syslog	HTTP status code events	Microsoft ISS Webserver logs	<a href="http://www.microsoft.com">www.microsoft.com</a>
	Exchange Server	2003	Syslog	Exchange mail and security events	Microsoft Exchange Server	<a href="http://www.microsoft.com">www.microsoft.com</a>
	IAS Server	Windows 2000/2003	Syslog	All relevant events	Microsoft IAS Server	<a href="http://www.microsoft.com">www.microsoft.com</a>
	Windows Event Security Log	2000/XP	Syslog	All relevant events	Microsoft Security Event Log	<a href="http://www.microsoft.com">www.microsoft.com</a>
	SQL Server	2000/2005	Syslog	Mail and security events	Microsoft SQL Server	<a href="http://www.microsoft.com">www.microsoft.com</a>
	DHCP Server	2000/2003	Syslog	All relevant events	Microsoft DHCP Server	<a href="http://www.microsoft.com">www.microsoft.com</a>
Niksun	NetVCR 2005	v3.x	Syslog	All relevant Niksun events	Niksun 2005 v3.5	<a href="http://www.niksun.com">www.niksun.com</a>
Nokia	Firewall	NG FP1, FP2, FP3, AI R54, AI R55, NGX on IPSO v3.8 and above	Syslog	All relevant events	Check Point Firewall-1	<a href="http://www.nokia.com">www.nokia.com</a>
	VPN-1	NG FP1, FP2, FP3, AI R54, AI R55, NGX on IPSO v3.8 and above	Syslog	All relevant events	Check Point Firewall-1	<a href="http://www.nokia.com">www.nokia.com</a>
	OPSEC	NG FP1, FP2, FP3, AI R54, AI R55, NGX on IPSO v.8 and above	OPSEC	All relevant events	Check Point Firewall-1	<a href="http://www.nokia.com">www.nokia.com</a>
Nortel	Contivity 5000	5000 V04_85.160, v6.0	Syslog	All relevant events	Nortel Contivity 5000 V04	<a href="http://www.nortel.com">www.nortel.com</a>

**Table 2-1** Supported DSMs (continued)

<b>Manufacturer</b>	<b>DSM</b>	<b>Versions Supported</b>	<b>Events Accepted</b>	<b>STRM Recorded Events</b>	<b>Option in STRM</b>	<b>For More Information</b>
	Application Switch	v3.2 and above	Syslog	All relevant status and network condition events	Nortel Application Switch	<a href="http://www.nortel.com">www.nortel.com</a>
	Contivity Firewall/VPN		Syslog	All relevant events	Nortel Contivity VPN Switch	<a href="http://www.nortel.com">www.nortel.com</a>
	ARN	15.5	Syslog	All relevant events	Nortel Advanced Remote Node (ARN) Router	<a href="http://www.nortel.com">www.nortel.com</a>
	VPN Gateway	v6.0 and above	Syslog	All relevant events	Nortel VPN Gateway	<a href="http://www.nortel.com">www.nortel.com</a>
	Switched Firewall 5100	4.1.4.1	Syslog or SNMP	All relevant events	Nortel Switched Firewall 5100	<a href="http://www.nortel.com">www.nortel.com</a>
	Switched Firewall 6000	4.1.4.1	Syslog or SNMP	All relevant events	Nortel Switched Firewall 6000	<a href="http://www.nortel.com">www.nortel.com</a>
Open Source	SNORT	v2.x	Syslog	All relevant events	Snort Open Source IDS	<a href="http://www.snort.org/docs">www.snort.org/docs</a>
Oracle	Audit Records	v9i and v10g	Syslog	All relevant Oracle events	Oracle RDBMS 9i/10g Audit Records	<a href="http://www.oracle.com">www.oracle.com</a>
	ProFTPD	v1.2.x, v1.3.x	Syslog	All relevant events	ProFTPD Server	<a href="http://www.proftpd.org">www.proftpd.org</a>
Secure Computing	Sidewinder G2	v61	Syslog	All Sidewinder events	Sidewinder G2 Security Appliance	<a href="http://www.securecomputing.com">www.securecomputing.com</a>
SonicWALL	UTM/Firewall/VPN Appliance	v3.x and above	Syslog	All relevant events	SonicWALL UTM/Firewall/VPN device	<a href="http://www.sonicwall.com">www.sonicwall.com</a>
SourceFire	Intrusion Sensor	IS 500, v2.x, 3.x, 4.x	Syslog	All relevant Sourcefire events	Snort Open Source IDS	<a href="http://www.sourcefire.com">www.sourcefire.com</a>
Sun	Solaris	v5.8, v5.9, Sun OS v5.8, v5.9	Syslog	All relevant events	Solaris Operating System Authentication Messages	<a href="http://www.sun.com">www.sun.com</a>
	Solaris DHCP	v2.8	Syslog	All relevant events	Solaris Operating System DHCP Logs	<a href="http://www.sun.com">www.sun.com</a>
	Solaris Sendmail	v2.x	Syslog	All relevant events	Solaris Operating System Sendmail Logs	<a href="http://www.sun.com">www.sun.com</a>

**Table 2-1** Supported DSMs (continued)

<b>Manufacturer</b>	<b>DSM</b>	<b>Versions Supported</b>	<b>Events Accepted</b>	<b>STRM Recorded Events</b>	<b>Option in STRM</b>	<b>For More Information</b>
Squid	Web Proxy	v2.6	Syslog	All cache and access log events	Squid WebProxy	<a href="http://www.squid-cache.org">www.squid-cache.org</a>
Symantec	SGS Appliance	v3.x and above	Syslog	All relevant events	Symantec Gateway Security (SGS) Appliance	<a href="http://www.symantec.com">www.symantec.com</a>
	SSC	v10.1	Syslog	All relevant events	Symantec System Center	<a href="http://www.symantec.com">www.symantec.com</a>
TippingPoint	UnityOne	v1.4 to v2.2	Syslog	All relevant events	TippingPoint Intrusion Prevention System (IPS)	<a href="http://www.tippingpoint.com">www.tippingpoint.com</a>
	SMS	v1.4 to v2.2	Syslog	All relevant events	TippingPoint Intrusion Prevention System (IPS)	<a href="http://www.tippingpoint.com">www.tippingpoint.com</a>
	X505/X506	v2.5 and above	Syslog	All relevant events	TippingPoint X Series Appliances	<a href="http://www.tippingpoint.com">www.tippingpoint.com</a>
TopLayer	IPS 5500	v4.1 and above	Syslog	All relevant events	Top Layer Intrusion Prevention System (IPS)	<a href="http://www.toplayer.com">www.toplayer.com</a>
Trend Micro	InterScan VirusWall	v6.0 and above	Syslog	All relevant events	Trend InterScan VirusWall	<a href="http://www.trendmicro.com">www.trendmicro.com</a>
Tripwire	Enterprise Manager	v5.2	Syslog	Resource additions, removal, and modification events	Tripwire Enterprise	<a href="http://www.tripwire.com">www.tripwire.com</a>
Vericept	Content 360	Up to v8.0	Syslog	All relevant events	Vericept Content 360	<a href="http://www.vericept.com">www.vericept.com</a>