



Security Threat Response Manager

Managing Sensor Devices

Release 2008.2 R2

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 530-027301-01, 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 2008.2 R2

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

September 2008—Revision 1

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

CONTENTS

ABOUT THIS GUIDE

Conventions	1
Audience	1
Technical Documentation	1
Contacting Customer Support	2

1 MANAGING SENSOR DEVICES

Configuring STRM Log Management to Receive Events	3
Managing Sensor Devices	4
Adding a Sensor Device	4
Editing Sensor Devices	6
Enabling/Disabling Sensor Devices	9
Deleting a Sensor Device	9
Configuring Protocols	10
Adding a Protocol	10
Editing a Protocol	17
Deleting a Protocol	17
Grouping Sensor Devices	18
Viewing Sensor Devices Using Groups	18
Creating a Group	18
Editing a Group	19
Copying a Sensor Device to Another Group	20
Removing a Sensor Device From a Group	20

2 CREATING A DEVICE EXTENSION

About Device Extensions	23
Creating a Device Extension Document	24
Viewing Device Extensions	24
Adding a Device Extension	25
Editing a Device Extension	27
Copying a Device Extension	28
Deleting a Device Extension	29
Enabling/Disabling a Device Extension	30
Reporting a Device Extension	30




ABOUT THIS GUIDE

The *Managing Sensor Devices Guide* provides you with information for configuring sensor devices (DSMs) in the STRM Log Management interface and integrating the DSMs with STRM Log Management.

Conventions

[Table 1](#) lists conventions that are used throughout this guide.

Table 1 Icons

Icon	Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, device, or network.
	Warning	Information that alerts you to potential personal injury.

Audience

This guide is intended for the system administrator responsible for setting up STRM Log Management in your network. This guide assumes that you have STRM Log Management administrative access and a knowledge of your corporate network and networking technologies.

Technical Documentation

You can access technical documentation, technical notes, and release notes directly from the Juniper Networks support web site at <https://juniper.net/support>. Once you access the Juniper Networks support web site, locate the product and software release for which you require documentation.

Your comments are important to us. Please send your e-mail comments about this guide or any of the Juniper Networks documentation to:

documentation@juniper.net

Include the following information with your comments:

- Document title
- Page number

**Contacting
Customer Support**

To help you resolve any issues that you may encounter when installing or maintaining STRM Log Management, you can contact Customer Support as follows:

- Log a support request 24/7: <https://juniper.net/support/>
For access to the Juniper Networks support web site, please contact Customer Support.
- Access Juniper Networks support and Self-Service support using e-mail: support@juniper.net
- Telephone assistance: 1-800-638-8296

1

MANAGING SENSOR DEVICES

You can configure STRM Log Management 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 Log Management with these external devices. This chapter provides information on configuring sensor devices to the system including:

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

Configuring STRM Log Management to Receive Events

STRM Log Management allows you to automatically discover sensor devices in your deployment that are sending syslog messages. Any sensor devices that are automatically discovered by STRM Log Management 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 Log Management Administration Guide*, Using the Deployment Editor.

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

Step 1 Configure the device to send events to STRM Log Management.

For information on configuring DSMs, see the *Configuring DSMs Guide* and your vendor documentation.

Step 2 Configure STRM Log Management to receive events from specific devices. See [Managing Sensor Devices](#).



Note: You must have administrative privileges to configure sensor devices in STRM Log Management. For more information on accessing the Administration Console, see the *STRM Log Management 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 the 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
LinuxServer @ qafedora		Linux login messages	true	qafedora	Syslog :: default syslog	eventcollector0 :: veyron	5	true
Pix @ apophis		Cisco PIX Firewall	true	apophis	Syslog :: default syslog	eventcollector0 :: veyron	5	true
Snort @ wolverine		Snort Open Source IDS	true	wolverine	Syslog :: default syslog	eventcollector0 :: veyron	5	true

- 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 :: veyron

Coalescing Events: Yes

Store Event Payload: Yes

Device Extension:

Extension Use Condition: Parsing Enhancement

Please select any groups you would like this device to be a member of:

- Step 4** Enter values for the parameters:

Table 1-1 Add 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 Adding a Protocol .
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 Log Management. Otherwise, STRM Log Management 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 STRM Settings 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 Log Management 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 STRM Settings 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 Log Management Administration Guide</i> .

Table 1-1 Add a Sensor Device Parameters

Parameter	Description
Device Extension	Using the drop-down list box, select the device extension you wish to use for this sensor device. Device extensions allow you to immediately extend the parsing routines of specific devices, which ensures DSMs send valid data to STRM. For more information on device extensions, see Creating a Device Extension .
Extension Use Condition	Using the drop-down list box, select the extension use condition that you wish to use for this sensor device: <ul style="list-style-type: none"> • Parsing Enhancement - When the DSM is unable to parse correctly or is unable to retrieve specific information from the DSM, the selected device extension overrides the failed parsing by the DSM. This is the default setting. • Parsing Override - When the DSM parses correctly for most fields, but needs either one or two fields corrected, the incorrectly parsed field values are enhanced.
Groups	Select any groups of which you wish this sensor device to be a member.

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.

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

Step 3 Select the sensor device you wish to edit.

Step 4 Click **Edit**.
The Edit a sensor device window appears.

Edit a sensor device
?

Device Name	<input type="text" value="LinuxServer @ qafedora"/>
Sensor Device Type	Linux login messages
Protocol Configuration	Syslog :: default syslog ▾
Device Description	<input type="text" value="LinuxServer device"/>
Device Hostname/IP	<input type="text" value="qafedora"/>
Credibility	5 ▾
Target Event Collector	eventcollector0 :: veyron ▾
Coalescing Events	Yes ▾
Store Event Payload	Yes ▾
Device Extension	▾
Extension Use Condition	Parsing Enhancement ▾

Please select any groups you would like this device to be a member of:

Step 5 Edit values for the parameters, as necessary:

Table 1-2 Edit 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 Adding a Protocol .
Device Description	Specify a description for the sensor device (optional).
Device Hostname/IP	Specify the hostname or IP address for the device.
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.

Table 1-2 Edit a Sensor Device Parameters (continued)

Parameter	Description
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 STRM Settings 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 Log Management 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 STRM Settings 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 Log Management Administration Guide</i>.</p>
Device Extension	<p>Using the drop-down list box, select the device extension you wish to use for this sensor device.</p> <p>Device extensions allow you to immediately extend the parsing routines of specific devices, which ensures DSMs send valid data to STRM.</p> <p>For more information on device extensions, see Creating a Device Extension.</p>
Extension Use Condition	<p>Using the drop-down list box, select the extension use condition that you wish to use for this sensor device:</p> <ul style="list-style-type: none"> • Parsing Enhancement - When the DSM is unable to parse correctly or is unable to retrieve specific information from the DSM, the selected device extension overrides the failed parsing by the DSM. This is the default setting. • Parsing Override - When the DSM parses correctly for most fields, but needs either one or two fields corrected, the incorrectly parsed field values are enhanced.
Groups	Select any groups of which you wish this sensor device to be a member.

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
LinuxServer @ qafedora		Linux login messages	true	qafedora	Syslog :: default syslog	eventcollector0 :: veyron	5	true
Pix @ apophis		Cisco PIX Firewall	true	apophis	Syslog :: default syslog	eventcollector0 :: veyron	5	true
Snort @ wolverine		Snort Open Source IDS	true	wolverine	Syslog :: default syslog	eventcollector0 :: veyron	5	true

- Step 3** Select the sensor device that 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 device by accessing Protocol Configuration or Sensor Devices in the SIM Configuration tab of the Administration Console.

The following procedures provide information on configuring protocols using the Protocol Configurations icon in the SIM Configuration panel.

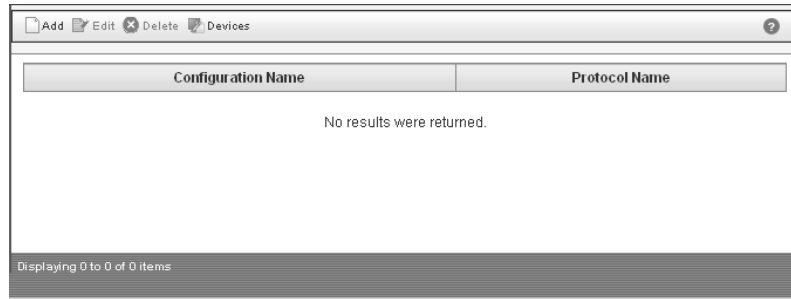
Using the Administration Console, you can:

- 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.

Add a protocol configuration

Configuration Name

Protocol

- 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.

The screenshot shows a dialog box titled "JDBC Configuration Parameters" with a subtitle "JDBC". The dialog contains the following fields and values:

- Database Type: MSDE (dropdown menu)
- Database Name: (empty text box)
- Table Name: (empty text box)
- Select List: *
- Compare Field: (empty text box)
- Hostname: (empty text box)
- Port: 1433
- Username: (empty text box)
- Password: (empty text box)
- Polling Interval: 10

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

- 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.

SiteProtector

IP

Port

Username

Password

Database Name

Table Name

- 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 IBM Proventia Management 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.

Juniper NSM Configuration Parameters ?

Juniper NSM

IP or Hostname

Inbound Port

Redirection Listen Port

Use NSM Address for Event Source

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.

OPSEC LEA Configuration Parameters ?

LEA

Server IP or Hostname

Server Port

Use Server IP for Event Source

Statistics Report Interval

Authentication Type

OPSEC Application Object SIC Attribute (SIC Name)

Log Source SIC Attribute (Entity SIC Name)

Specify Certificate

Certificate Authority IP or Hostname

Pull Certificate Password

OPSEC Application

- 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.
 - **Use 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.
 - **Statistics Report Interval** - Specify the interval, in seconds, during which the number of syslog events are recorded in the qradar.log file. The default is 600.
 - **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`.
The following parameters appear if `sslca` (SSL Certificate Authority) or `sslca_clear` is selected as the authentication type.
 - **OPSEC Application Object SIC Attribute (SIC Name)** - Specify the Secure Internal Communications (SIC) name of the OPSEC Application Object. The SIC name is the distinguished name (DN) of the application, for example:
`CN=LEA, o=fwconsole..7psasx`
 - **Log Source SIC Attribute (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, for example:
`cn=cp_mgmt, o=fwconsole..7psasx`
 - **Specify Certificate** - Select the check box if you wish to specify a certificate for this LEA configuration. STRM Log Management attempts to retrieve the certificate using these parameters when the certificate is required. If you select the check box, the following parameter appears:
Certificate Filename - This option only appears if Specify Certificate is selected. 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 and above), 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.

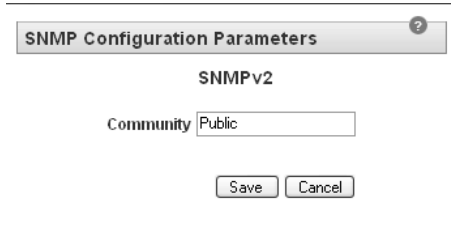
- c Click **Save**.

The Protocol Configurations window appears.

Step 11 If you have selected SNMPv2:

- a Click **Configure**.

The SNMPv2 Configuration Parameters window appears.



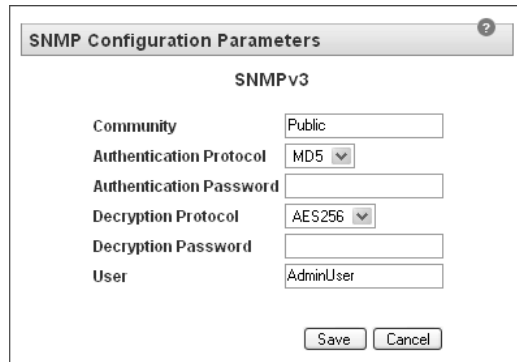
- b In the Community field, specify the SNMP community, such as public. This parameter only applies if you are using SNMPv2c. The default is Public.
- c Click **Save**.

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 Log Management Administration Guide*.

This section provides information on grouping reports including:

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

Viewing Sensor Devices Using Groups

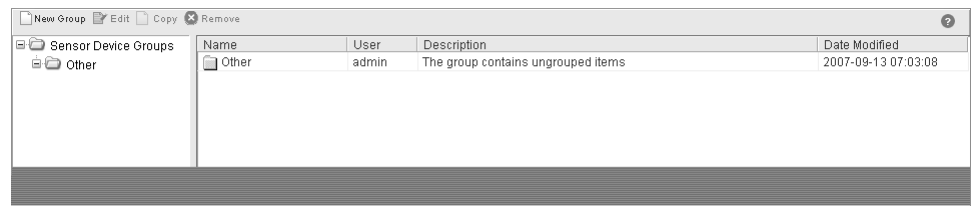
To view sensor devices using groups:

- 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.



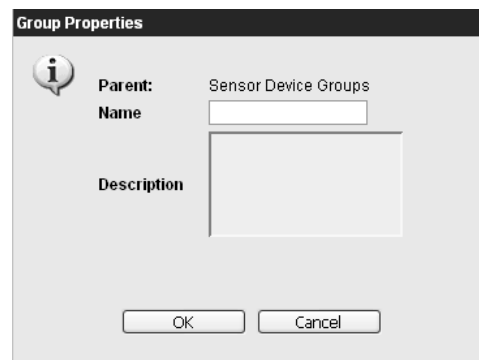
Step 3 From the menu tree, select the group under which you wish to create a new group.



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.



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 Sensor Device Groups tree, select the group from which you wish to copy the sensor device.

A list of sensor devices appears in the Group Content Frame.

Step 4 From the Group Content Frame, select the sensor device(s) you wish to copy to another group.

Step 5 Click **Copy**.

The Choose Group window appears.

Step 6 Select the group(s) to which you wish to copy the sensor device.

Step 7 Click **Assign Groups**.

Step 8 Close the Groups window.

Removing a Sensor Device From a Group

To remove 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 Log Management.

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 a group with items to be removed.

Step 4 From the Group Content Frame, select the item(s) you wish to remove.

Step 5 Click **Remove**.

A confirmation window appears.

Step 6 Click **OK**.

Step 7 Close the Groups window.

2

CREATING A DEVICE EXTENSION

Device extensions allow you to immediately extend the parsing routines of specific devices. For example, you can use a device extension to detect an event that has missing or incorrect fields or a device extension can parse an event when the DSM to which it is attached fails to produce a result.



Note: For information on configuring sensor devices, see the [Managing Sensor Devices](#) chapter.

This chapter includes information on configuring a device extension including:

- [About Device Extensions](#)
- [Creating a Device Extension Document](#)
- [Viewing Device Extensions](#)
- [Adding a Device Extension](#)
- [Editing a Device Extension](#)
- [Copying a Device Extension](#)
- [Deleting a Device Extension](#)
- [Enabling/Disabling a Device Extension](#)
- [Reporting a Device Extension](#)

About Device Extensions

A device extension allows a DSM to parse logs even if the DSM has not received an update to the DSM. Information about device extensions is accessed from the STRM Log Management Administration Console.

You can also create device extension reports that can be sent to Juniper Networks Customer Support. This capability is a mechanism for reporting parsing issues and potential fixes to Juniper Networks Customer Support, so that they can be evaluated for inclusion in future DSM updates.

Creating a Device Extension Document

Before defining a device extension within STRM Log Management, you must build the extension document. The extension document is an XML document that you create or edit using any common word processing application. Multiple extension documents can be created, uploaded, and associated to various device types.

The format of the extension document must conform to a standard XML schema document (XSD).



Note: For more information on creating an extensions document, see *Using Extension Documents Technical Note*.

The name of the extension document must be in the following format:

`<filename>.xml`

When you select an extension document for uploading, STRM Log Management validates it against the internal XSD before it is uploaded. If the file is not a valid document, it is not uploaded. The following is an example of a valid device extension document:

```
<?xml version="1.0" encoding="UTF-8" ?>
<device-extension xmlns="event_parsing/device_extension">
  <pattern id="EventName" xmlns=""> <![CDATA[ %FWSM[a-zA-Z\-\]*\d-(\d{1,6}) ]]> </pattern>
  <pattern id="SourceIp" xmlns=""> <![CDATA[gaddr
(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]> </pattern>
  <pattern id="EventNameId" xmlns=""><![CDATA[(\d{1,6})]]></pattern>
  <match-group order="1" description="FWSM Test" device-type-id-override="6" xmlns="">
    <matcher field="EventName" order="1" pattern-id="EventName" capture-group="1"
      enable-substitutions="false" />
    <matcher field="SourceIp" order="1" pattern-id="SourceIp" capture-group="1" />
    <event-match-multiple pattern-id="EventNameId" capture-group-index="1"
device-event-category="Cisco Firewall" severity="7" send-identity="OverrideAndNeverSend" />
  </match-group>
</device-extension>
```

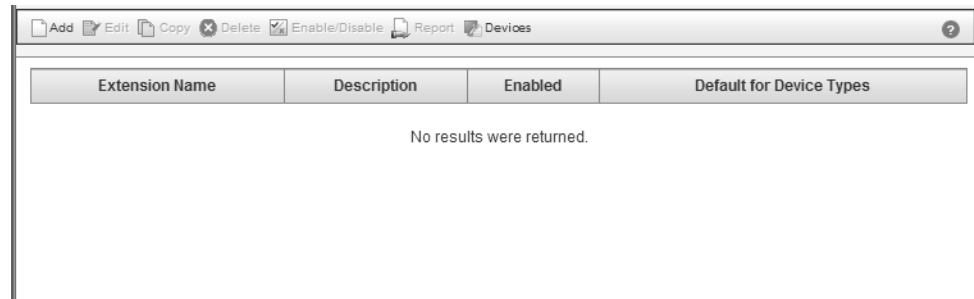


Note: To develop an extension document, knowledge of and experience with XML coding is required.

Viewing Device Extensions

To view the configured device extensions:

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



The Device Extensions window provides the following details for each device extension:

Table 2-1 Device Extension Parameters

Parameter	Description
Extension Name	Specifies the name of the device extension.
Description	Specifies a description for this device extension.
Enabled	Specifies whether or not the device extension is enabled.
Default for Device Types	Specifies the device type(s) for which the device extension is the default.

Adding a Device Extension

To add a device extension:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.
The SIM Configuration panel appears.
- Step 2** Click the **Sensor Device Extensions** icon.
The Device Extensions window appears.
- Step 3** Click **Add**.
The Add a Device Extension window appears.

Add a Device Extension ?

Name

Description

Use Condition Parsing Enhancement ▼

Sensor Device Types

Available

3Com 8800 Series Switch
AmbironTrustWave ipANGEL Intrusion Prevention
Array Networks SSL VPN Access Gateways
Bluecoat SG Appliance
Check Point FireWall-1

Set to default for

⇨
⇨

Upload Extension: Browse... Upload

Save
Cancel

Step 4 Enter values for the parameters:

Table 2-2 Add Device Extension Parameters

Parameter	Description
Name	Specify a name for the device extension. The name can be a maximum of 255 alphanumeric characters plus the underscore (_).
Description	Specify a description for the device extension. The description can be a maximum of 255 characters.
Use Condition	Using the drop-down list box, select one of the following: <ul style="list-style-type: none"> • Parsing Enhancement - When the DSM is unable to parse correctly and is unable to retrieve specific information from the DSM, the device extension overrides the failed parsing by the DSM. This is the default. • Parsing Override - When the DSM parses correctly for most fields, but needs either one or two fields corrected, the incorrectly parsed field values are enhanced.
Sensor Device Types Available	Select a device type and click the right arrow to have the new device extension marked as the default device extension for that device. Repeat this step for each device type for which you want the device extension to be the default. If you do not associate a device extension to a device type or a specific device, it will not be used.

Step 5 Click **Browse** and locate a device extension document (<filename>.xml) to be uploaded.

Step 6 Click **Upload**.

A non-editable, XML-formatted extension script appears in the Extension Document box.

Step 7 Click **Save**.

The new device extension is created. The Event Collector automatically detects changes and will pick up a new or revised device extension.

By default new device extensions are enabled. If you want to disable the device extension, see [Enabling/Disabling a Device Extension](#).



Note: If you want to report the device extension document back to Juniper Networks Customer Support, see [Reporting a Device Extension](#).

Editing a Device Extension

This section provides information on how to edit a device extension, such as modifying the definition of a device extension or changing the device to which it is the default device extension.

To edit a device extension:

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

The SIM Configuration panel appears.

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

The Device Extensions window appears.

Step 3 From the list of device extensions, select the device extension that you want to edit.**Step 4** Click **Edit**.

The Edit a Device Extension window appears.

Extension Document

```
<device-extension xmlns="http://www.juniper.com/products/sern/device_extension">
  <pattern xmlns="" id="EventName">%FWSM[a-zA-Z]*%-(\d{1,6})</pattern>
  <match-group xmlns="" description="FWSM Test" order="1" device-type-id-override="6">
    <matcher capture-group="1" enable-substitutions="false" pattern-id="EventName" order="1" field="EventName" />
    <matcher capture-group="1" pattern-id="SourceIp" order="1" field="SourceIp" />
    <event-match-multiple capture-group-index="1" pattern-id="EventName" device-event-category="Cisco Firewall" severity="7" send-identity="OverrideAndNeverSend" />
  </match-group>
</device-extension>
```

Step 5 Update parameters, as necessary:

Table 2-3 Edit Device Extension Parameters

Parameter	Description
Name	Specify the name for the device extension. The name can be a maximum of 255 alphanumeric characters plus the underscore (_).
Description	Specify the description for the device extension. The description can be a maximum of 255 characters.
Use Condition	Using the drop-down list box, select one of the following: <ul style="list-style-type: none"> • Parsing Enhancement - When the DSM is unable to parse correctly and it is unable to retrieve specific information from the DSM, the device extension overrides the failed parsing by the DSM. This is the default setting. • Parsing Override - When the DSM parses correctly for most fields, but needs either one or two fields corrected, the incorrectly parsed field values are enhanced.
Sensor Device Types Available	Select a device type and click the right arrow to have the device extension marked as the default device extension for that device. Repeat this step for each device type for which you want the device extension to be the default.
Sensor Device Types Set to default for	Select a device type and click the left arrow to remove that device from the list of devices for which the device extension is the default. Repeat this action for each device type for which you do not want the device extension to be the default.

Step 6 Click **Browse** and locate a device extension document (<filename>.xml) if you want to upload an extension document to replace the existing extension document, and click **Upload**.

Step 7 Click **Save**.

The device extension is changed. The Event Collector automatically detects changes and will pick up a new or revised device extension.

Copying a Device Extension

This section provides information on how to copy a device extension. Use this function if you want to create a new device extension that has some or all of the parameters of an existing device extension. You can use an existing device extension as a template.

To copy a device extension:

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

The SIM Configuration panel appears.

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

The Device Extensions window appears.

Step 3 From the list of device extensions, select the device extension that you want to copy.

Step 4 Click **Copy**.

The Copy a Device Extension window appears.

Step 5 Enter values for the parameters:

Table 2-4 Copy Device Extension Parameters

Parameter	Description
Name	Specify a name for the device extension. The name can be a maximum of 255 alphanumeric characters plus the underscore (_).
Description	Specify a description for the device extension. The description can be a maximum of 255 characters.
Use Condition	Using the drop-down list box, select one of the following: <ul style="list-style-type: none"> • Parsing Enhancement - When the DSM is unable to parse correctly and is unable to retrieve specific information from the DSM, the device extension overrides the failed parsing by the DSM. This is the default setting. • Parsing Override - When the DSM parses correctly for most fields, but needs either one or two fields corrected, the incorrectly parsed field values are enhanced.
Sensor Device Types Available	Select a device type and click the right arrow to have the new device extension marked as the default device extension for that device. Repeat this step for each device type for which you want the device extension to be the default.

Step 6 Click **Save**.

The new device extension is created. The Event Collector automatically detects changes and enforces the new device extension.

Deleting a Device Extension

To delete a device extension:

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

The SIM Configuration panel appears.

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

The Device Extensions window appears.

Step 3 From the list of device extensions, select the device extension that you want to delete.

Step 4 Click **Delete**.

A confirmation window appears.

Step 5 Click **Yes** to confirm the deletion.

Step 6 Click **Save**.

Enabling/Disabling a Device Extension

If you want to enable an existing device extension or disable an existing device extension (without deleting it), this section provides information on how to enable and disable a device extension.

To enable or disable a device extension:

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

The SIM Configuration panel appears.

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

The Device Extensions window appears.

Step 3 From the list of device extensions, select the device extension that you want to enable or disable.

Step 4 Click **Enable/Disable**.

The status (true or false) appears in the Enabled column.

Step 5 Click **Save**.

The new device extension is changed. The Event Collector automatically detects changes and enforces the revised device extension.

Reporting a Device Extension

After you create a device extension, you have the option of sending information about that device extension to Juniper Networks Customer Support. Sending this information to Juniper Networks Customer Support facilitates the process of providing you with support.

To send a report of the device extension to Juniper Networks Customer Support:

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

The SIM Configuration panel appears.

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

Step 3 From the list of device extensions, select the device extension that you want to send to Juniper Networks Customer Support.

Step 4 Click **Report**.

The Report Device Extensions menu appears with the extension document in the Extension Document field.

Report Device Extension

Customer Name

Technical Contact Name

Comments

Extension Name

Extension Document

```
<device-extension xmlns="http://www.q1labs.com/products/sem/device_extension">
  <pattern xmlns="" id="1">some crazy regex -- we need to test a bunch of these</pattern>
  <match-group xmlns="" order="1" description="test group">
    <matcher order="1" capture-group="" pattern-id="1" field="EventName" />
    </matcher order="1" capture-group="1" pattern-id="1" field="EventName" />
  </match-group>
</device-extension>
```

Step 5 Enter values for the parameters:

Table 2-5 Reporting a Device Extension Parameters

Parameter	Description
Customer Name	Specify your company's or organization's name
Technical Contact Name	Specify the name of the technical contact
Comments	Specify any comments that may be useful in understanding the issue

Step 6 Click **Send**.

