



RSA | Security Analytics

Event Source Management
for Version 10.6.5

Contact Information

RSA Link at <https://community.rsa.com> contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

October 2017

Contents

About Event Source Management	7
Prerequisites	7
Navigate to Event Source Management	7
Alarms and Notifications	9
Large Email Notifications	10
High and Low Thresholds Both Triggered	10
Automatic Alerting	12
Common Scenarios for Monitoring Policies	13
Manage Event Source Groups	15
Definitions	15
Manage Tab Details	15
Default Groups	16
Create Event Source Groups	17
Procedure	17
Examples	18
Simple Example	18
Complex Example	20
Edit or Delete Event Source Groups	21
Edit an Event Source Group	21
Delete an Event Source Group	21
Create an Event Source and Edit Attributes	23
Mandatory Attributes	23
Create an Event Source	24
Update Attributes for an Event Source	24
Bulk Edit Event Source Attributes	26
Import Event Sources	28
Import Event Source Attributes	28

Troubleshooting the Import File	30
Export Event Sources	31
Sort Event Sources	33
Monitor Policies	35
Configure Event Source Group Alerts	36
Create an Alert Policy for an Event Source Group	36
Set and View the Thresholds for an Alert Policy	37
Set Up Notifications	39
Prerequisites	39
Add Notifications for an event source group	39
Disable Notifications	42
Prerequisites	42
Disable Notifications	42
View Event Source Alarms	43
Sort the Alarms Information	43
Filter Alarms by Type	44
Configure Automatic Alerting	45
Prerequisites	45
Configure Automatic Alerting	45
Event Source Management Reference	47
Alarms Tab	48
Event Sources View	51
Manage Tab	52
Groups Panel	52
Event Sources Panel	54
Sorting	55
Monitoring Policies Tab	57
Event Groups Panel	58
Thresholds Panel	58

Notifications Panel	59
Create/Edit Group Form	64
Parameters	64
Rule Criteria	64
Settings Tab	67
About Automatic Alerting	67
Features	68
Manage Event Source Tab	70
Features	70
Categories	71
Troubleshoot Event Source Management	75
Alarms and Notifications Issues	76
Alarms	76
Automatic Alarms	76
Manual Alarms	76
Notifications	76
Automatic Notifications	76
Manual Notifications	77
Duplicate Log Messages	78
Details	78
Clean Up Duplicate Messages	78
Exporting Event Source Issues	79
Issue	79
Guidelines	79
Process	79
Import Options	80
Tip	80
Troubleshoot Feeds	81
Details	81
How it Works	81
Feed File	81
Troubleshooting Feeds	82

10.5 Log Decoders	82
Feed File Existence	82
Group Meta Populated on LD	82
Device Group Meta on Concentrator	83
SMS Log File	83
Verify Logstats data is getting Read & Published by ESMReader & ESMAggregator	84
Configure JMX Feed Generator Job Interval	87
Import File Issues	88
Negative Policy Numbering	89
Details	89
Clean Up Duplicate Messages	89

About Event Source Management

The Event Source module in Security Analytics provides an easy way to manage event sources and configure alerting policies for your event sources.

Prerequisites

There are two permissions that affect Event Source Management:

- **View Event Sources** is needed for users to view event sources, their attributes, and their thresholds and policies.
- **Modify Event Sources** allows users to add, edit, and otherwise update event sources.

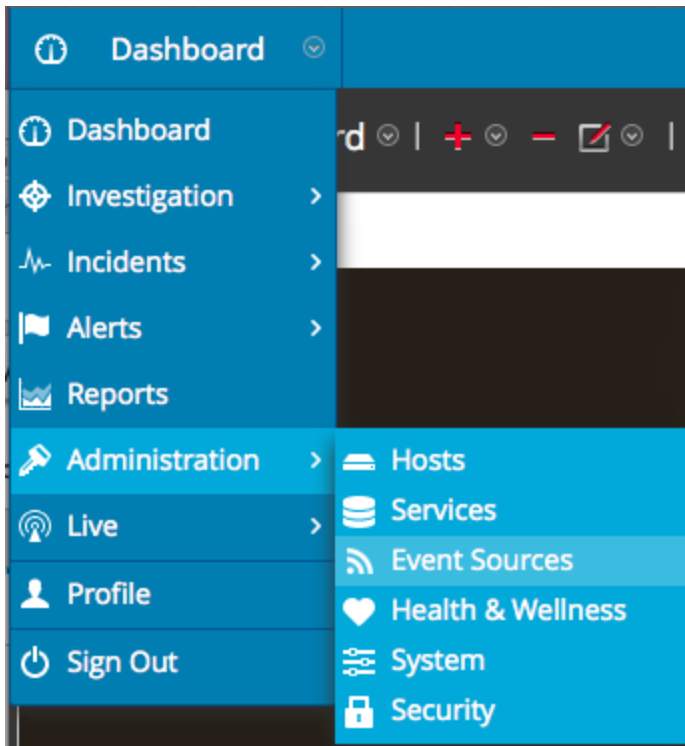
For details, see the following topics:

- The *Roles Tab* topic available in the **System Security and User Management** guide > **References** > **Administration Security View** > **Roles Tab**.
- The *Role Permissions* topic describes the built-in Security Analytics system roles, which control access to the user interface. Available in the **System Security and User Management** guide > **How Role-Based Access Control Works**.
- The *Manage Users with Roles and Permissions* topic describes how to manage users in Security Analytics, using roles and permissions. Available in the **System Security and User Management** guide > **Manage Users with Roles and Permissions**.

Navigate to Event Source Management

You can view the details about your existing event source groups by doing the following:

1. In the **Security Analytics** menu, select **Administration > Event Sources**.



2. Click any of the following:

- The **Manage** tab. This tab provides the details for your existing event source groups.
- The **Monitoring Policies** tab. Use this tab to view or edit your event source alerting configuration.
- The **Alarms** tab. Use this tab to see the details of the alarms that have been generated. Alarms are generated when event sources exceed or fall below their set thresholds.
- The **Settings** tab. Use this tab to view or change the behavior for automatic alerts.

Note: When the system receives logs from an event source that does not currently exist in the Event Source List, Security Analytics automatically adds the event source to the list. Additionally, if it matches the criteria for any existing group, it becomes part of that group.

Alarms and Notifications

The Event Source module in Security Analytics displays alarms and sends notifications based on alarms that are triggered.

For alarms, consider the following:

Alarms are of two types: **automatic** (triggered when baselines are exceeded or not met) and **manual** (configured using thresholds).

- **Automatic:** If you turn on automatic alerts, the system reports alarms for **all** event sources that go above or below their normal baselines by the required amount. You can specify the over / under percentage on the [Settings Tab](#).
- **Manual:** If you turn off automatic alerts, you receive alarms only for the event source groups for which you have specified—and enabled—policies (and thresholds).
- Alarms appear on the UI, in the [Alarms Tab](#).

For notifications, consider the following:

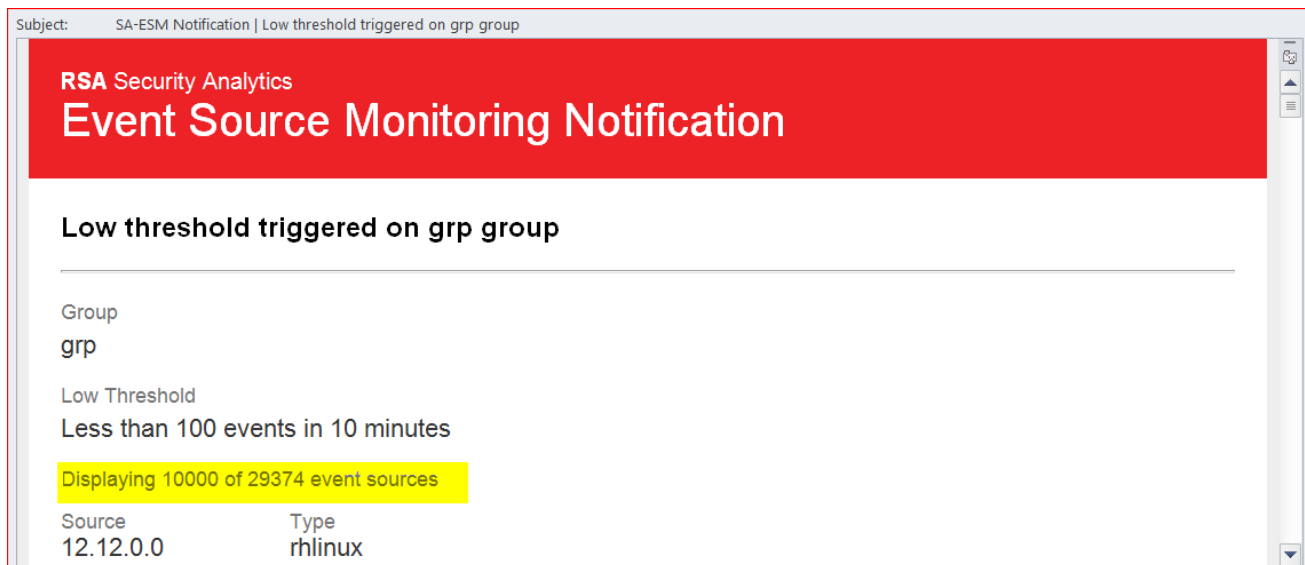
- To receive manual notifications (via email, SNMP or Syslog):
 - Specify a policy for an event source group.
 - Set a high or low (or both) threshold.
 - Enable the policy.
- To receive automatic (baseline) notifications:
 - Baseline alerting must be on. This is turned on by default.
 - You must enable notifications from automatic monitoring. See [Configure Automatic Alerting](#) for details.
 - The event source that triggers the alarm must be in a group that has a policy enabled.
- If you have automatic alerting turned on, and you have configured a policy and threshold for a group:
 - If the event source goes outside its baseline, you see an automatic alert and receive a notification.
 - If the event source goes outside its thresholds, you see a manual alert and receive a notification.

- If both occur (threshold and baseline exceeded or not met), you receive two alarms (visible on the Alarms tab) and a notification that indicates both alarms. That notification will list the event source that double alarmed twice; one listing indicating it was an automatic alarm.

Large Email Notifications

If you have set up email notifications, keep in mind that the email can grow very large, depending on the number of event sources in the notification.

If the number of event sources in the alarmed state exceeds 10,000, then the email notification contains the details for only the first 10,000 and a total count. This is to ensure that the email is successfully delivered.



High and Low Thresholds Both Triggered

There may be occasions when both the high and low alarms are both triggered for a particular event source group. The easiest way to see when this happens is to read the email header, which clearly states when both thresholds are triggered, as shown in this image:

RSA Security Analytics

Event Source Monitoring Notification

High threshold and Low threshold triggered on ciscopix group

Group

ciscopix

High Threshold

Greater than 250 events in 60 minutes

In this example, the header states, "High threshold and Low threshold triggered on ciscopix group." To see the details for the low threshold event sources, you may need to scroll down past hundreds, or even thousands, of the high threshold event sources.

Automatic Alerting

This topic describes automatic alerts, which are based on baseline settings.

Note: Automatic alerting, and all of the parameters that determine its behavior, are currently in Beta testing.

You can set up policies and thresholds for your event source groups. You do this so that you receive notifications when the thresholds are not met. Security Analytics also provides an automatic way to receive alarms, if you do not want to set up thresholds to generate alarms.

To trigger automatic alerts, you can use baseline values. This way, you do not need to set up numerous group thresholds and policies in order to receive alerts. Any anomalous amount of messages trigger alerts, without needing to do any configuration (except for turning on automatic alerting).

Note the following:

- Once you begin collecting messages from an event source, it takes the system approximately a week to store a baseline value for that event source. After this initial period, the system alerts you when the number of messages for a period are above or below the baseline by a set amount. By default, this amount is 2 standard deviations above or below the baseline.
- Base your high and low deviation settings on how "regular" your event sources behave. That is, if you expect little or no variance in the number of messages that arrive for a given time (for example, 8 to 9 am on a weekday), then you can set a low value for the Deviation. Conversely, if you often see peaks and valleys, set the Deviation value higher.
- If you enable a policy, but do not have any thresholds set, then you can still receive automatic (baseline) notifications, as long as you have turned on automatic alerting.

Common Scenarios for Monitoring Policies

Typically, organizations monitor their event sources in "buckets" based on how critical the event sources are. One typical example is as follows:

- There is a group of PCI devices, and it is critical to know if any of these devices stop sending messages (or send too few messages) within a half hour.
- There is a group of Windows devices, and it is useful to know if any of these devices stop sending messages after four hours.
- There is a group of quiet devices that do not typically send a lot of messages, but you would like to know if they do not send anything for 24 hours.

Many organizations may have a network that resembles this example. You may have more or different categories, but this example is used to discuss this feature.

You may have dozens or even hundreds of event source groups, and still only have a few groups for which you need to set thresholds and alerts.

Note: If an Event Source is a member of multiple groups that have alerting configured, it will only alert on the first matching group in the ordered list. (The Monitor Policies tab presents an ordered list of your groups.)

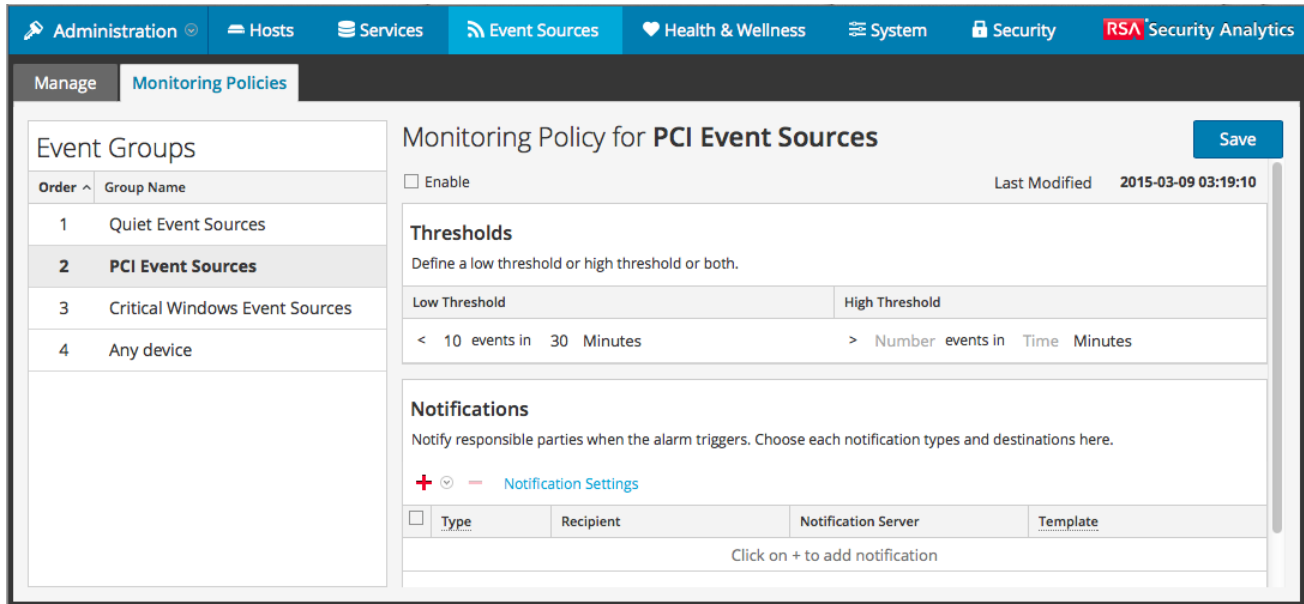
Ordering the Groups

Note: To change the order of the groups, drag and drop a group to its new location. The higher a group is listed, the higher the precedence for that group's thresholds: RSA Security Analytics checks the thresholds in the order provided in this panel. Thus, your highest priority groups should be at the top of this list.

The first thing to keep in mind is how to order your groups on the Monitoring Policies page. Assuming that you have the three groups mentioned above, you should order them as follows:

1. Quiet event sources. Having this group first ensures that you will not get numerous false alerts.
2. High priority PCI event sources. The highest priority devices should be after the quiet devices
3. Windows event sources. The time range is longer (four hours versus a half hour) for these devices than for the PCI devices. Therefore, they should come after the PCI devices.

- All event sources. Optionally, you could set thresholds for all devices as a catch-all. This ensures that your entire network is operating as expected. For the catch-all group, you do not need to specify any thresholds—you can use automatic alerting to generate alarms for the event sources in this group.



In the figure above, note the following:

- The groups are ordered as discussed in the previous section.
- The threshold for PCI devices is to alert if the number of messages coming in to Security Analytics is fewer than 10 messages in 30 minutes.
- A low threshold is defined, but not a high threshold. This is typical for many use cases.

After you have set up and ordered your groups and begun to receive alerts, you may need to adjust the order. Use these guidelines to help you adjust the ordering:

- If you receive more notifications than you need, you can move the group down in the order. Similarly, if you are getting too few notifications, move the group up towards the top.
- If you notice that one event source is creating more alerts than it should, you can move it to another group, or create a new group for that event source.

Manage Event Source Groups

Definitions

When dealing with event source groups in Security Analytics, note the following:

- An **event source** is essentially the combination of values for all of its attributes.
- An **event source group** is the set of event sources that match a set of criteria that are defined for that group.

For example, you might have the following groups:

- A group named **Windows Devices**, consisting of all the event source types associated with Microsoft Windows event sources (`winevent_nic`, `winevent_er`, and `winevent_snare`).
- A group named **Low Priority Services**, consisting of all services where the Priority attribute has been set lower than 5.
- A group named **U.S. Sales Servers**, where you gather event sources located in the U.S.A. and having an Organization attribute of Sales, Finance, or Marketing.

Manage Tab Details

The Manage tab in the Event Source module provides an easy way to manage event sources. In this tab, you can:

- Set up event source groups in a consistent way.
- Work with event source attributes in a consistent, straightforward manner.
- Easily search through your entire set of event sources.
- Bulk edit and update your event sources and event source groups.

You can view the details about your event source groups by doing the following:

1. In the **Security Analytics** menu, select **Administration > Event Sources**.
2. Select the **Manage** panel to see the details for your existing event source groups.

Note: When the system receives logs from an event source that does not currently exist in the Event Source List, Security Analytics automatically adds the event source to the list. Additionally, if it matches the criteria for any existing groups, it becomes part of that group.

Default Groups

RSA Security Analytics has several default groups. You can customize these as required and use them as templates for creating new groups.

The default groups are as follows:

- All Event Sources
- All Unix Event Sources
- All Windows Event Sources
- Critical Windows Event Sources
- PCI Event Sources
- Quiet Event Sources

You can edit any of these groups to investigate the rules that define the groups.

Note: You cannot edit or delete the **All** event source group.

Create Event Source Groups

Administrators must receive notifications when event sources are no longer being collected by Security Analytics. They need to be able to configure how long the event sources can be quiet (that is, not collect any log messages) before sending a notification based on different factors.

RSA Security Analytics provides event source groups so that you can group similarly important devices together. You can create groups based on attributes that you imported from your CMDB (configuration management database), or by manually choosing event sources to add to the group.

For example, these are some of the types of event source groups that you can create:

- PCI sources
- Windows Domain Controllers
- Quiet sources
- Finance Servers
- High Priority devices
- All Windows sources

Procedure

To create an Event Source group:

1. In the **Security Analytics** menu, select **Administration > Event Sources**.
2. In the **Manage** panel, click **+**.

The Create an Event Group dialog is displayed.

Create an Event Group

Group Name * McAfee Event Sources

Description Group containing all of the monitored McAfee event sources on the system.

Conditions * All of these + -

Add one or more conditions.

Cancel Save

3. Enter a Group Name.
4. Enter a Description.
5. Click **+** to add a condition. Continue adding conditions as necessary. For details on constructing conditions, see [Create/Edit Group Form](#).
6. Click **Save**.

The new group is listed in the **Manage** panel.

Examples

This section describes a simple example, and then discusses how to set up a more complex set of rules.

Simple Example

If you want to create an event source group that contains all of your high priority event sources, this example describes the necessary steps.

1. In the **Security Analytics** menu, select **Administration > Event Sources**.
2. In the **Manage > Groups** panel, click **+**.
3. Enter **High Priority Devices** for the Group Name.
4. Enter a description, such as, "These devices are our highest priority ones, and must be monitored closely."
5. Leave **All of these** selected and click **+** to add a condition.
6. Select **Add condition** from the drop-down menu.
 - a. Select an Attribute: **Priority**.
 - b. Select an Operator: **Less than**.
 - c. Enter a value: **2**.

The following figure displays the updated Edit Event Group dialog.

The screenshot shows the 'Edit Event Group' dialog box. The 'Group Name' field is filled with 'High Priority Devices'. The 'Description' field contains the text 'These devices are our highest priority ones, and must be monitored closely.'. Under the 'Conditions' section, the 'All of these' option is selected in the dropdown menu. A '+' button is visible next to the dropdown. Below this, there is a checkbox, a dropdown menu with 'Priority' selected, another dropdown menu with 'Less than' selected, and a text input field containing the number '2'. At the bottom right of the dialog, there are 'Cancel' and 'Save' buttons.

7. Click **Save**.

Complex Example

In this example, you want to create a fairly complex rule: match event sources that are in the United States, and in either the Sales, Finance, or Marketing departments. Also, match worldwide internal, high priority Sales event sources. High Priority is assumed to be where the priority is 1 or 0. Logically, the definition is as follows:

```
(Country=United States AND (Dept.=Sales OR
Dept.=Finance OR Dept.=Marketing))
OR
(Priority < 2 AND Division != External AND
Dept.=Sales)
```

The following figure is an example of the criteria for creating such an Event Source Group.

The screenshot shows the 'Edit Event Group' dialog box with the following configuration:

- Group Name ***: US Marketing or US Finance or Worldwide High Priority Sales
- Description**: Event sources in the US and Sales/Finance/Marketing, or high priority (Priority is 0 or 1) Internal Sales
- Conditions ***:
 - Any of these
 - All of these
 - Country = United States
 - Department = Sales, Finance, Marketing
 - All of these
 - Priority < 2
 - Division != External
 - Department = Sales


Edit or Delete Event Source Groups

You may occasionally need to remove an event source group. For example, if you close an office, and you had a group consisting of all the event sources in that office, you can remove the group, since none of those event sources will send information to Security Analytics.

Similarly, you may need to change some of the conditions that are used to populate the group.

Note: You cannot edit the event source group name. Once you create a group, that name exists as long as the group itself exists.

Edit an Event Source Group

1. In the **Security Analytics** menu, select **Administration > Event Sources**.
2. In the **Manage** panel, select an existing Event Source Group.
3. Click  .
The Edit Event Group dialog is displayed.
4. Modify any of the details, or add, edit or remove conditions as necessary.
5. Click **Save**.

Delete an Event Source Group

Note the following:

- You can delete any group except for the **All** group, which lists all configured event sources in the system.
- If you delete a group, the associated policy for that group also gets deleted automatically.
- If there are any event sources that belong **only** to the deleted group, they would no longer have a policy alarm associated with them. Remember that event sources can belong to multiple groups.
- Deleting a group has no effect on baseline alarms.

To delete an event source group:

1. In the **Security Analytics** menu, select **Administration > Event Sources**.
2. In the **Manage** panel, select an existing Event Source Group.

3. Click .

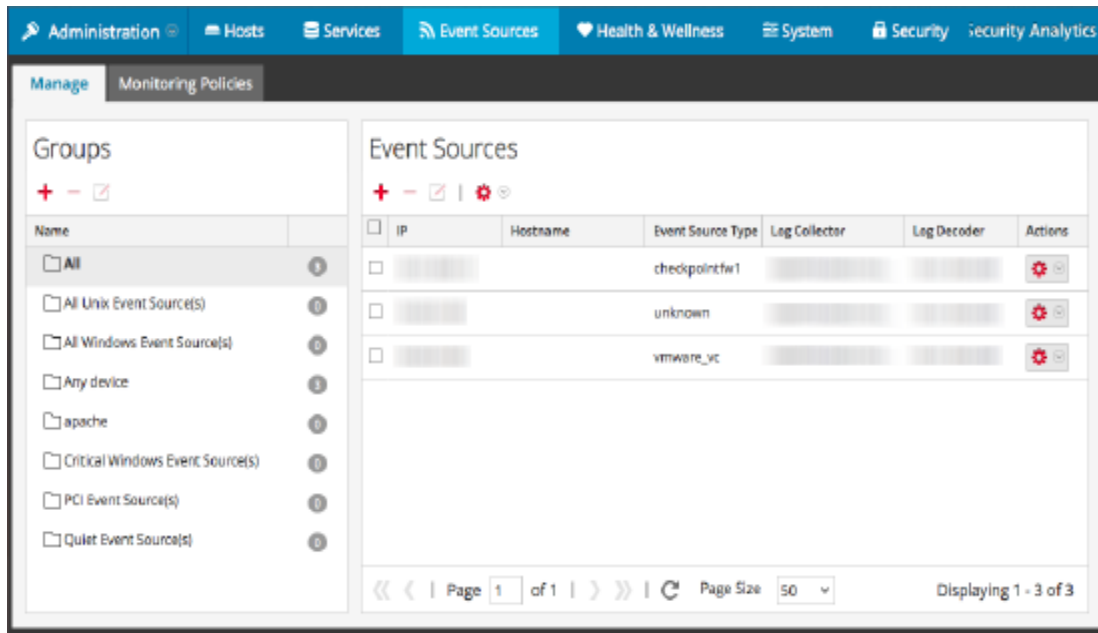
A confirmation dialog is displayed.

4. Click **Yes** to delete the group.

Create an Event Source and Edit Attributes

You can organize your event sources into groups. You do this by entering values for various attributes for each event source. For example, for all of your high priority event sources, you could set the **Priority** to 1. You can see details about the available attributes on the [Manage Event Source Tab](#).

The following figure shows an example of the Event Sources panel:



Event source attributes are a combination of auto-populated and user-entered information. When an event source sends log information to Security Analytics, it is added to the list of event sources, and some basic information is auto-populated. At any time after that, users can add or edit details for other event source attributes.

Mandatory Attributes

The following identification attributes are handled specially: **IP**, **IPv6**, **Hostname**, **Event Source Type**, **Log Collector**, and **Log Decoder**. If you create an event source manually, you can enter these values. Once you save the event source, these values can no longer be changed.

Event sources can also be auto-discovered; any event source that sends messages to the Log Decoder will be added to the list of event sources. If you edit the attributes for an auto-discovered event source, you cannot edit any of these fields.

Note that not all of these fields are mandatory. To uniquely identify an event source, the following information is required:

- IP or IPv6 or Hostname, and
- Event Source Type

Additionally, RSA Security Analytics uses a hierarchy for IP, IPv6, and Hostname. The order is as follows:

1. IP
2. IPv6
3. Hostname

If you enter event sources manually, then you need to keep this order in mind, otherwise, you may end up with duplicates when messages are received from the event sources that you manually added.

All other attributes (such as Priority, Country, Company, Vendor, and so on) are optional.


Create an Event Source

1. In the **Security Analytics** menu, select **Administration > Event Sources**.
2. Select the **Manage** tab.
3. In the **Event Sources** panel, click **+** to open the details screen, which contains all of the event source attributes.

The [Manage Event Source Tab](#) is displayed.

4. Enter or change the values for any attributes.
5. Click **Save**.

Update Attributes for an Event Source

1. In the **Security Analytics** menu, select **Administration > Event Sources**.
2. Select the **Manage** tab.
3. In the **Event Sources** panel, select an event source from the list.
4. In the **Event Sources** panel, click  to open the details screen, which contains all of the event source attributes.

The [Manage Event Source Tab](#) is displayed.

5. Enter or change the values for any attributes, except for certain attributes that cannot be

altered once entered.

6. Click **Save**

Bulk Edit Event Source Attributes

You can select multiple event sources, or an entire group, or even all event sources for bulk editing. For example, you might want to change the Priority or the Manager for a large number of your event sources.

Note: You cannot select individual event sources across displayed pages. For example, if you have a group with 225 event sources, and your Page Size is 50, you can only select event sources from the currently displayed 50 items.

If you want to edit items that span multiple pages, you can do the following:

- In the browser, increase the page size (the maximum is 500 entries on a single page). If your page size is small, you might be able to get all of your items on a single page.
- Create a new event source group that contains only the items that you want to bulk edit. Then, you can select all items for that group, rather than selecting individual items.
- Bulk edit incrementally. On the first page, select the items that you want to edit. Make your edits, then go to the next page and repeat the process, until you have made all of your changes.

Bulk Edit Attributes

Note: Mandatory fields cannot be edited; IP, IPv6, Hostname, Event Source Type, Log Collector, and Log Decoder.

To bulk edit attributes for Event Sources:

1. In the **Security Analytics** menu, select **Administration > Event Sources**.
2. Select the **Manage** tab.
3. Optionally, select an event source group.
4. In the **Event Sources** panel, select one or more event sources to edit.

Note: To select all event sources, select the box next to the **Actions** column in the last (far-right) column of the list table.

5. Select the **Edit** icon  from the menu bar.

The Bulk Edit Event Source dialog is displayed.

The screenshot shows a 'Bulk Edit Event Source' dialog box. It features a title bar with a close button. The main content is organized into sections: 'Properties' (with fields for Name, DNS Hostname, and Description, where Description is checked and contains 'High Priority Devices'), 'Importance' (with fields for Priority, Criticality, and Compliance, where Priority is checked and contains '1'), and a partially visible 'Zone' section. At the bottom, there are 'Cancel' and 'Save' buttons.

6. Enter values for any of the available attributes. In the screen shot above, the Name and Priority attributes have been updated.
7. When you have updated as many attributes as required, click **Save**.

Import Event Sources

You can import event source attributes from a CSV-formatted file. To import information from a configuration management database (CMDB), a spreadsheet, or other type of file, first convert or save the information to a CSV file.

Note: The following identification attributes are handled specially: **IP**, **IPv6**, **Hostname**, **Event Source Type**, **Log Collector**, and **Log Decoder**. If you import an event source that includes a different value for any of these fields (when compared with the value in Security Analytics), the original value in Security Analytics will **not** be overwritten.

The imported attributes are associated with the matched Event Source and are available for use in rules to create Event Source Groups.

RSA Security Analytics treats the import file as the correct, complete record. This assumption leads to the following behaviors related to importing event source attributes:

- By default, when you import attributes, the system updates attributes for existing event sources only.
- If the event source exists in the import file, but not in Security Analytics, the attributes for that event source are ignored. That is, Security Analytics does **not** create a new event source for these attributes.
- If the event source exists in both the import file and Security Analytics, values for that event source are overwritten.
- If an attribute is blank in the import file, it clears the corresponding attribute in Security Analytics.
- If an attribute is not specified in the import file, then the corresponding attribute is ignored in Security Analytics (that is, it is **not** cleared).

Note: There is a difference between a blank attribute vs. one that is not specified at all. If an attribute is specified but blank, the assumption is that it is meant to be blank, and Security Analytics clears that attribute for the corresponding event source. However, if an attribute is not specified at all, it is assumed that no change is expected.

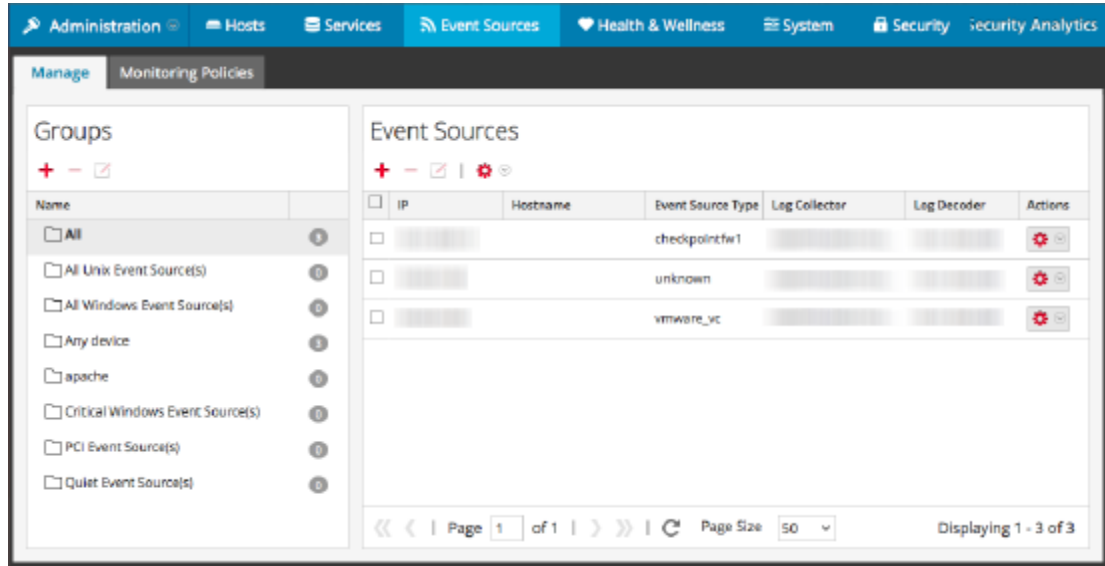
The above behaviors are the defaults—you can change the behavior as specified in the following procedure.



Import Event Source Attributes

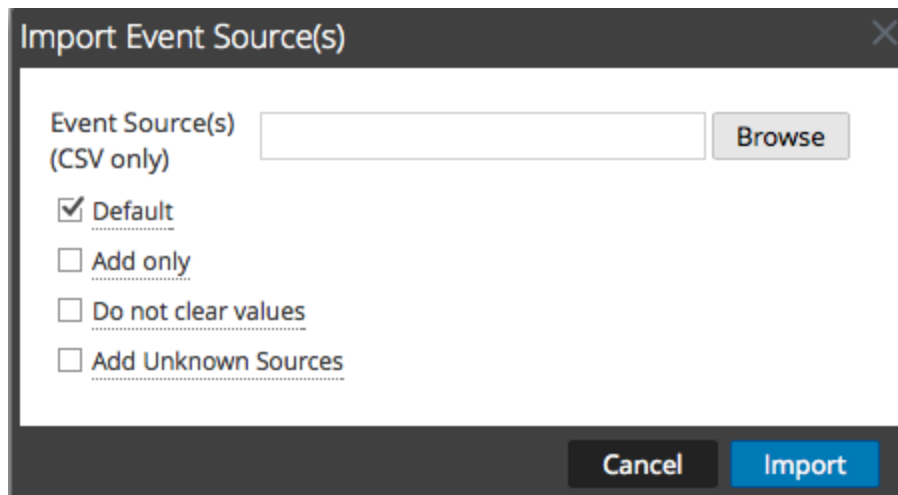
To import Event Source attributes from a file:

1. In the **Security Analytics** menu, select **Administration > Event Sources**.
2. Select the **Manage** tab.

The Event Sources Manage tab is displayed.



3. From the Import/Export menu in the toolbar (), select **Import** ( **Import**).
The Import Event Sources dialog is displayed.



4. Navigate to the import file, and select the appropriate boxes:
 - **Default:** The default behavior is described above.
 - **Add only:** Imports an attribute only if the corresponding field in Security Analytics is blank. Thus, no existing values will be overwritten.

- **Do not clear values:** Does not clear attribute values in Security Analytics for items in the import file that are blank.
- **Add Unknown Sources:** Adds new event sources based on items in the import file.

Note: You can select multiple options.

5. Click **Import**.
6. Click **Yes** in the confirmation dialog to perform the import.

Troubleshooting the Import File

If your import file is not formatted correctly, or is missing required information, an error is displayed, and the file is not imported.

Check the following:

- If you are adding unknown sources, each line in the file must contain a combination of the required attributes:
 - IP or IPv6 or Hostname, and
 - Event Source Type
- The first line of the file must contain header names, and the names must match the names in Security Analytics. To get a list of correct column names, you can export a single event source. Examine the exported CSV file: the first row of the file contains the correct set of attribute/column names.

Export Event Sources

You can export all or some of your event sources, along with their corresponding attributes, to a CSV file.

Note the following:

- The exported CSV includes all attribute columns.
- The exported CSV includes a header line at the top, listing each column name.
- You can export all entries in a group.
- You can export all entries (select the **All** group).
- You can select entries and export only those entries.

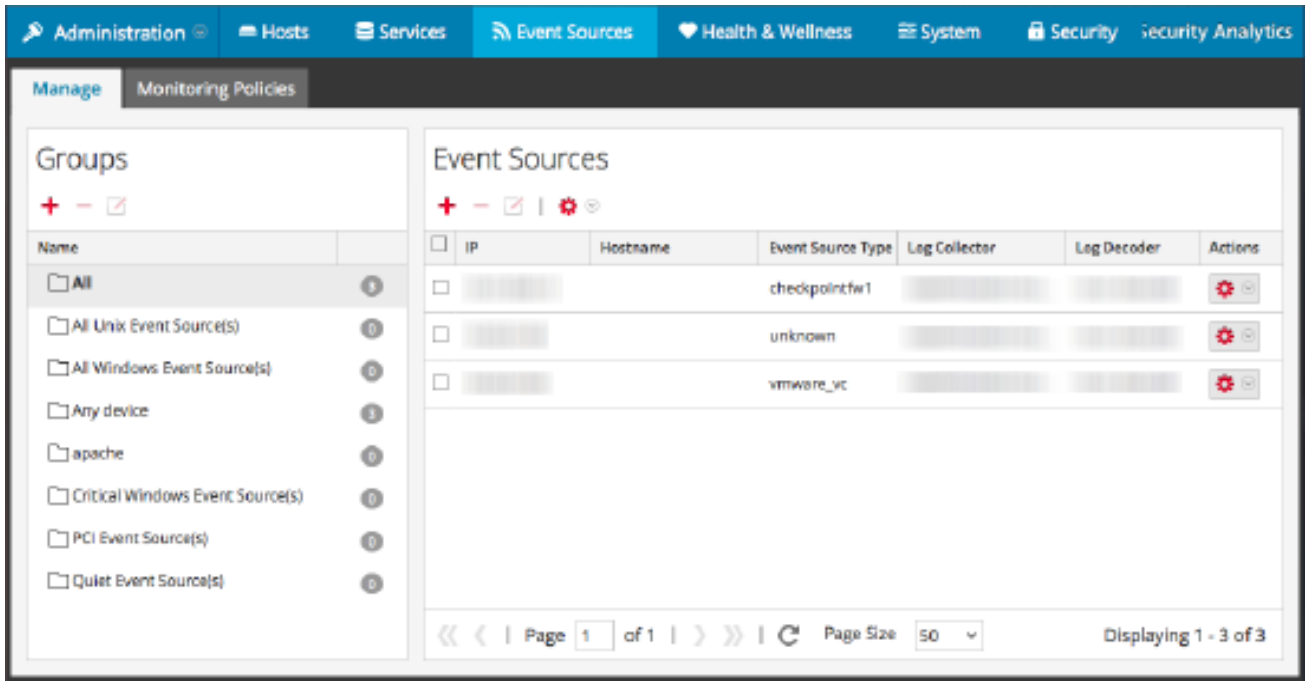
Warning: When using a spreadsheet program to edit an exported event source CSV file, some data fields like numbers and dates can be re-formatted into the spreadsheet program's native field types. This can cause issues when re-importing this information, as some data fields may be garbled or formatted incorrectly. This can be avoided by importing the CSV file into the spreadsheet program, and specifying all data fields as text values.


Export Event Sources

To export your Event Sources:

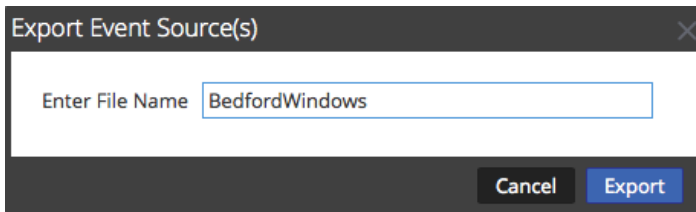
1. In the **Security Analytics** menu, select **Administration > Event Sources**.
2. Select the **Manage** tab.

The Event Sources Manage tab is displayed.



3. Select the group that contains the event sources to export.
4. Select as many event sources as you need. Alternatively, you can export the entire group: to export the entire group, you do not need to select any individual event sources.
5. From the Import/Export menu in the toolbar (), select **Export (.csv)** or **Export Group (.csv)**.

The Export Event Sources dialog is displayed.



6. Enter a file name and click export.ddd

The event source attributes are saved to the file name you specified, in a CSV format.

Sort Event Sources

The event sources panel displays attributes for the currently selected event source group. You can configure the list of attributes that are displayed, as well as sort the list on any of the displayed attributes.

Note the following behaviors when sorting event sources:

- The entire list is sorted, not just the items displayed on the current page. (The navigation bar at the bottom of the page shows how many pages exist for this list of event sources.)
- The sort order is case sensitive. For any string column, if the values contains a mix of lower case and upper case, the upper case appears in the list before the lower case.

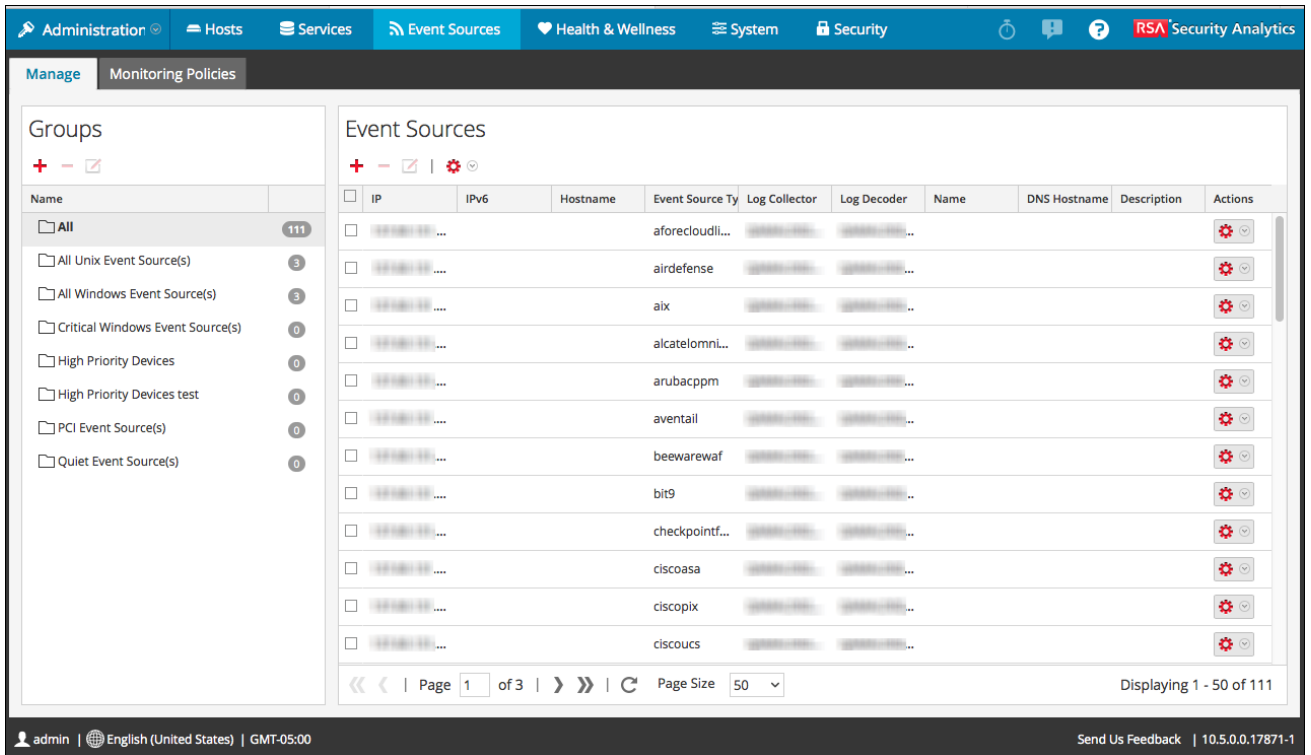
For example, assume the Event Source Type column contains the following entries: Netflow, APACHE, netwitnesspectrum, ciscoasa. The sort order would be as follows:


- APACHE
- Netflow
- ciscoasa
- netwitnesspectrum

To sort your event sources:

1. In the **Security Analytics** menu, select **Administration > Event Sources**.
2. Select the **Manage** tab.

The Event Sources Manage tab is displayed.



3. To sort a column, click  in the column header.
The Sort Options drop-down menu is displayed.
4. Select the sort order that you want.

Monitor Policies

Use the Monitoring Policies view to manage alert configuration for your event source groups.

You can create policies that alert on event source groups, by setting thresholds and notifications:

- Thresholds set ranges for frequency of log messages. You can specify a low threshold, a high threshold, or both.
- Notifications describe how and where to send alerts when thresholds are not met.
- You combine thresholds and notifications to create alerts based on the frequency you specify.
- If automatic alerting is enabled (it is by default), you can create and enable a policy *without* setting any thresholds. If you then turn on automatic notifications, notifications will be sent whenever an event source in the group is above or below its baseline by the specified amount.

For example, let's say that you have created an event source group that consists of all your Windows event sources based in the United Kingdom. You could specify a policy that alerts you whenever fewer than 1000 events per 30 minutes arrive.

Note: In addition to, or instead of setting up monitoring policies for your event source groups, you can [Configure Automatic Alerting](#) to view alarms when the number of messages for an event source are outside of the normal bounds.

Configure Event Source Group Alerts

Each event source group can have its own alerting policy. This includes setting the thresholds for when to alert, and setting the notification type when an alert is triggered. This topic describes the steps involved in creating an alert policy for an event source group.

Create an Alert Policy for an Event Source Group

1. In the **Security Analytics** menu, select **Administration > Event Sources**.
2. Select the **Monitoring Policies** tab.
3. In the **Event Groups** panel, select a group.
4. Enter values for the Low Threshold and High Threshold fields.

This is an example of alert thresholds.

Monitoring Policy for **PCI Event Source(s)** Save

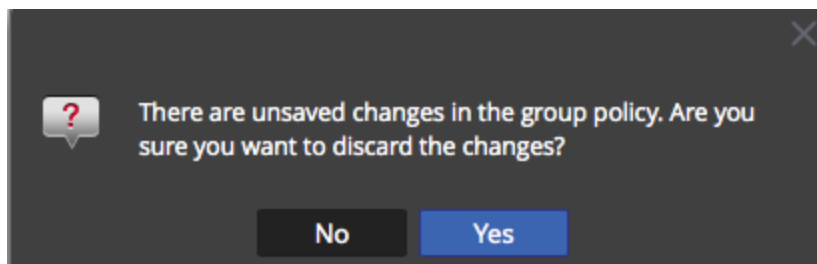
Enable Last Modified 2015-08-06 20:24:51

Thresholds
Define a low threshold or high threshold or both.

Low Threshold	High Threshold
< 40 events in 30 Minutes	> 500 events in 30 Minutes

5. Select **Enable** and click **Save** to enable the alert policy that you have configured.

Note: If you make changes to a policy, and attempt to exit the page before you save your changes, an Unsaved Changes warning message is displayed:



Set and View the Thresholds for an Alert Policy

Every event source group is also an alert policy. Thresholds are part of an alert policy. You can set thresholds for each alert policy. For each policy, you can set a low threshold, a high threshold, or both. Additionally, you can enable a policy without setting any thresholds; this allows you to receive notifications based on automatic alerts. Automatic alerts are generated when the baseline for an event source is out of normal bounds.

1. In the **Security Analytics** menu, select **Administration > Event Sources**.
2. Select the **Monitoring Policies** tab.
3. In the **Event Groups** panel, select a group.
Any thresholds set for the selected group are displayed in the **Thresholds** panel.

Monitoring Policy for PCI Event Source(s) Save

Enable Last Modified **2015-08-06 20:24:51**

Thresholds

Define a low threshold or high threshold or both.

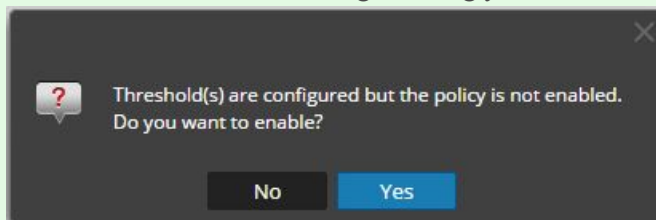
Low Threshold	High Threshold
< 40 events in 30 Minutes	> 500 events in 30 Minutes

4. Edit the values in either the Low or High Threshold as follows:
 - a. Enter the number of events for the threshold.
 - b. Enter the number of minutes or hours for the threshold. The minimum value is 5 minutes.

Note: For each threshold, you can set either the low values, the high values, or both.

5. Select **Enable** to enable alarms when thresholds are not met.

Note: If you configure a threshold and attempt to save the page without enabling it, you receive a confirmation message, asking you whether or not to enable the policy:



For example, suppose you enter 10 and 30 for the values for the low threshold: **10** events in **30** minutes, and 20 and 30 for the values for the high threshold: **20** events in **30** minutes. This means that you expect between 10 to 20 events are logged in 30 minutes (for the selected event source group). That is, anything between the low and high threshold is considered normal, and does not trigger an alarm.

Note: Once you add a threshold for a policy, you cannot delete it. You can disable the policy, or set the low or high threshold to 0 events in 5 minutes. Five minutes is the minimum duration for a threshold.

Set Up Notifications

This topic describes how to configure notifications for event source groups. Notifications are sent when thresholds are not met.

Notifications go hand-in-hand with Thresholds. Before you configure notifications, you should set up Thresholds for an event source group.

Note: After configuring the thresholds for an event source group, if you do not set any notifications, then even if an alarm is triggered, users are not notified. However, all alarms are visible on the [Alarms Tab](#).

Prerequisites

Before you set up notifications for an event source group, you should review the available notification items:

- **Notification Servers:** These are the servers that you want to receive notifications from the system. For more details, see the **Notification Servers Overview** topic in the *System Configuration Guide*.
- **Notification Templates:** These are the available templates for each type of notification. For Event Source Management, default templates are supplied for Email (SMTP), SNMP, and Syslog. You can use these templates as supplied, or customize them if necessary. For more details, see the **Templates Overview** topic in the *Systems Configuration Guide*.
- **Notification Output:** The outputs contain the parameters for the notification type. For example, an email notification type contains the email addresses and subject for the notification. For more details, see the **Notification Outputs Overview** topic in the *Systems Configuration Guide*.

Add Notifications for an event source group

To add notifications for an event source group:

1. In the **Security Analytics** menu, select **Administration > Event Sources**.
2. Select the **Monitoring Policies** tab.
3. In the **Event Groups** panel, select a group.

Note: You should have already set a threshold for the group. If not, see [Set and View the Thresholds for an Alert Policy](#) to set a threshold, and then return to this procedure. Alternatively, if you have automatic alerting turned on, then you do not need to set thresholds for a policy. Automatic alarms generate notifications without the need to set thresholds.

4. In the Notifications panel, click **+**, and from the drop-down menu, select the type of notification you want to add:
 - Email
 - SNMP
 - Syslog

Note: Default ESM (Event Source Monitoring) templates are provided for each type of notification.

5. Enter values for the Notification, Notification Server, and Template fields.
 - a. For Notification, select from the list, or add a suitable notification type in **Notifications**, and then select it here.
 - b. For the Server, select one from the list, or add a suitable server in **Notifications**, and then select it here.
 - c. For Template, select an available template, or create a suitable template in **Notifications**, and then select it here.

Note: If you need to add or edit one of these items, click **Notification Settings**. A new browser window opens on the **Administration > System > Global Notifications** page. Use this page to view or update the available Notification items.

6. Optionally, you can limit the rate of notifications for a policy.
 - a. Select **Output Suppression** to enable setting a limit.
 - b. Enter a value, in minutes, for the suppression rate. For example, if you enter **30**, notifications for this policy are limited to one notification every 30 minutes.
 - c. Click **Save**.

Here is an example of a monitoring policy that contains a threshold and notification for an event source group.

Monitoring Policy for **Quiet Event Source(s)** Save

Enable Last Modified **2015-08-06 20:24:51**

Thresholds

Define a low threshold or high threshold or both.

Low Threshold	High Threshold
< 10 events in 4 Hours	> 1000 events in 60 Minutes

Notifications

Notify responsible parties when the alarm triggers. Choose each notification type and destination here.

+ ▼ - [Notification Settings](#)

<input checked="" type="checkbox"/>	Output	Recipient	Notification Server	Template
<input checked="" type="checkbox"/>	EMAIL	test-email	test-email	ESM Default Email Template

Output Suppression of every minutes

Disable Notifications

Notifications are sent when thresholds are not met. Additionally, automatic notifications are sent when baselines are not met. However, you may determine that you no longer require notifications for the event sources in a particular group. In this case, you can disable notifications for the event source group.

Note: Even if you disable all notifications, the details for alarms are still visible on the [Alarms Tab](#).

Prerequisites

You must have configured thresholds and notifications for an event source group, and enabled them. For automatic notifications, you must have selected **Enable Notifications From Automatic Monitoring** on the [Settings Tab](#).

Disable Notifications

To disable notifications (both manual and automatic) for an event source group:


1. In the **Security Analytics** menu, select **Administration > Event Sources**.
2. Select the **Monitoring Policies** tab.
3. In the **Event Groups** panel, select a group.
4. Click **Enable** to remove the check mark. Clearing this option means that notifications are not sent for this event source group, even if thresholds are not met or exceeded.
5. Additionally, you can remove all notifications. However, this is not required to stop the notifications.

View Event Source Alarms

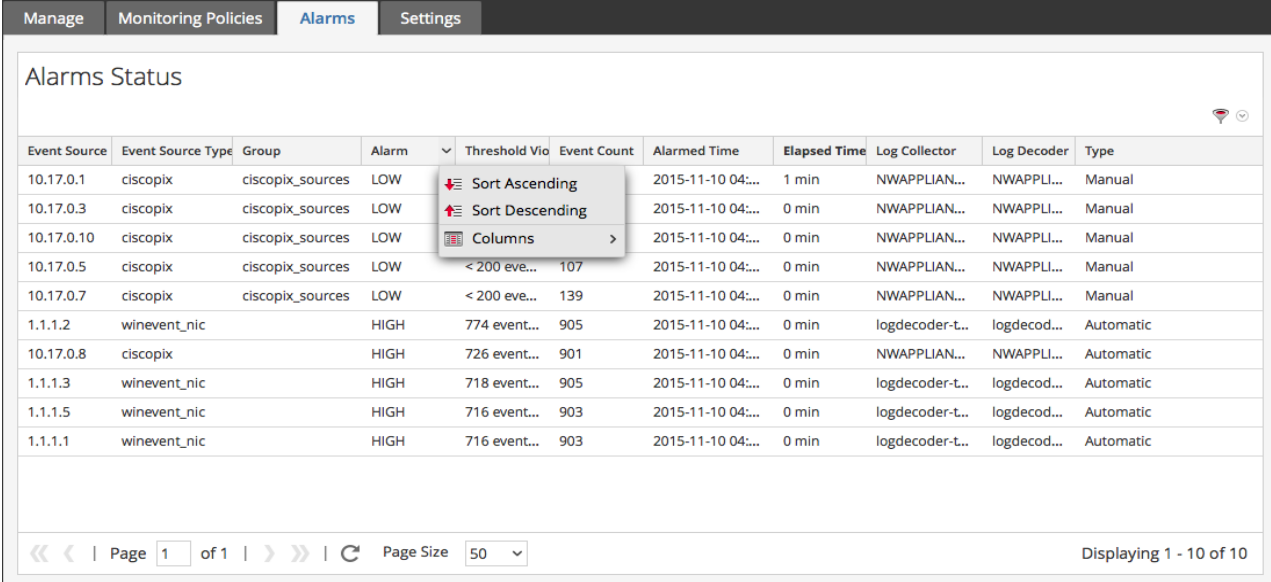
This topic describes how to view alarms for your event source groups. Once you have configured and set alerts, you can view all of the generated alarms in the **Alarms** tab of the **Event Sources** view.

Sort the Alarms Information

When you first access this view, the data is sorted by most recent alarm (the Alarmed time column). You can sort by any column.

1. In the **Security Analytics** menu, select **Administration > Event Sources**.
2. Mouse over a column that you want to sort.
3. Click the Select the **Alarms** tab.
4. Mouse over the column that you want sorted, and click the  icon.

This is an example when you mouse over the Alarm column.



Event Source	Event Source Type	Group	Alarm	Threshold Viol	Event Count	Alarmed Time	Elapsed Time	Log Collector	Log Decoder	Type
10.17.0.1	ciscopix	ciscopix_sources	LOW			2015-11-10 04:...	1 min	NWAPPLIAN...	NWAPPLI...	Manual
10.17.0.3	ciscopix	ciscopix_sources	LOW			2015-11-10 04:...	0 min	NWAPPLIAN...	NWAPPLI...	Manual
10.17.0.10	ciscopix	ciscopix_sources	LOW			2015-11-10 04:...	0 min	NWAPPLIAN...	NWAPPLI...	Manual
10.17.0.5	ciscopix	ciscopix_sources	LOW	< 200 eve...	107	2015-11-10 04:...	0 min	NWAPPLIAN...	NWAPPLI...	Manual
10.17.0.7	ciscopix	ciscopix_sources	LOW	< 200 eve...	139	2015-11-10 04:...	0 min	NWAPPLIAN...	NWAPPLI...	Manual
1.1.1.2	winevent_nic		HIGH	774 event...	905	2015-11-10 04:...	0 min	logdecoder-t...	logdecod...	Automatic
10.17.0.8	ciscopix		HIGH	726 event...	901	2015-11-10 04:...	0 min	NWAPPLIAN...	NWAPPLI...	Automatic
1.1.1.3	winevent_nic		HIGH	718 event...	905	2015-11-10 04:...	0 min	logdecoder-t...	logdecod...	Automatic
1.1.1.5	winevent_nic		HIGH	716 event...	903	2015-11-10 04:...	0 min	logdecoder-t...	logdecod...	Automatic
1.1.1.1	winevent_nic		HIGH	716 event...	903	2015-11-10 04:...	0 min	logdecoder-t...	logdecod...	Automatic

Navigation: Page 1 of 1 | Page Size 50 | Displaying 1 - 10 of 10

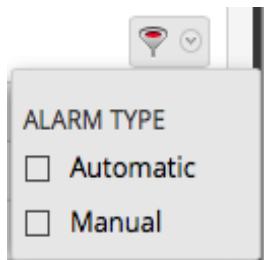
5. Select either **Sort Ascending** or **Sort Descending** to sort the column in the way you wish.

The data is sorted across all pages.

Note: You can also sort by two columns. To do this, first sort by the secondary column, then sort by the primary column. For example, if you want to see all the HIGH alarms by their group order, first sort on **Group**, then sort on **Alarm**.

Filter Alarms by Type

You can also filter the alarms by their type: you can display only the Manual or Automatic (baseline) alarms. To filter by alarm type, select the filter icon on the right side of screen, in the heading area:



Select either Automatic or Manual:

- If you select Automatic, only the alerts based on baselines are displayed.
- If you select Manual, only the alarms for which you have set thresholds are displayed.

Configure Automatic Alerting

Note: Automatic alerting, and its settings, are currently in Beta testing.

Prerequisites

Before you set up notifications for an event source group, you should review the available notification items:

- **Notification Servers:** These are the servers that you want to receive notifications from the system. For more details, see the **Notification Servers Overview** topic in the *System Configuration Guide*.
- **Notification Templates:** These are the available templates for each type of notification. For Event Source Management, default templates are supplied for Email (SMTP), SNMP, and Syslog. You can use these templates as supplied, or customize them if necessary. For more details, see the **Templates Overview** topic in the *Systems Configuration Guide*.
- **Notification Output:** The outputs contain the parameters for the notification type. For example, an email notification type contains the email addresses and subject for the notification. For more details, see the **Notification Outputs Overview** topic in the *Systems Configuration Guide*.

Configure Automatic Alerting

1. In the **Security Analytics** menu, select **Administration > Event Sources**.
2. Select the **Settings** tab.
The Settings tab is displayed.

Manage Monitoring Policies Alarms **Settings**

Automatic Monitoring Settings (Beta)

Adjust automatic event source monitoring settings and thresholds.

Monitoring Configuration

Enable Automatic Monitoring

Enable Notifications from Automatic Monitoring

Low Standard Deviations 2

High Standard Deviations 2

Enable Aggregation Persistence

Aggregation Persistence Interval in Days 120

Enable Generation of Analytics

Reset Apply

3. By default, automatic monitoring is turned on. To turn off automatic alerting, clear the **Enable Automatic Monitoring** option.
4. By default, notifications for automatic alerts is turned off. To turn on automatic notifications, select the **Enable Notifications From Automatic Monitoring** option.
5. Configure the parameters, based on your usage patterns:
 - **Low Standard Deviations:** standard deviations below which to receive alerts. Default is **2.0** (95% confidence).
 - **High Standard Deviations:** standard deviations above which to receive alerts. Default is **2.0** (95% confidence).

Note: You can adjust the standard deviation settings in increments of 0.1 (one tenth) of a standard deviation. vvv

6. Click **Save** to close the dialog and save your settings.

Event Source Management Reference

ESM Reference Topics:

- [Event Sources View](#)
- [Manage Tab](#)
- [Monitoring Policies Tab](#)
- [Alarms Tab](#)
- [Settings Tab](#)
- [Create/Edit Group Form](#)
- [Manage Event Source Tab](#)

Alarms Tab

The Alarms tab presents the details for Event Sources that are currently in violation of a policy and threshold. Only Event Sources in violation of a policy appear in the list. Once the event source returns to a normal state, the corresponding alarm disappears from the list.

To access this tab, in the **Security Analytics** menu, select **Administration > Event Sources > Alarms**.


Alarms Status											
Event Source	Event Source Type	Group	Alarm ^	Threshold Violated	Event Count	Alarmed Time	Elapsed Time	Last Updated Time	Log Collector	Log Decoder	Type
1.1.1.2	winevent_nic		HIGH	774 events abo...	905	2015-11-10 04:30:...	0 min	2015-11-10 04:...	logdecoder-t...	logdecod...	Automatic
10.17.0.8	ciscopix		HIGH	726 events abo...	901	2015-11-10 04:30:...	0 min	2015-11-10 04:...	NWAPPLIAN...	NWAPPLI...	Automatic
1.1.1.3	winevent_nic		HIGH	718 events abo...	905	2015-11-10 04:30:...	0 min	2015-11-10 04:...	logdecoder-t...	logdecod...	Automatic
1.1.1.5	winevent_nic		HIGH	716 events abo...	903	2015-11-10 04:30:...	0 min	2015-11-10 04:...	logdecoder-t...	logdecod...	Automatic
1.1.1.1	winevent_nic		HIGH	716 events abo...	903	2015-11-10 04:30:...	0 min	2015-11-10 04:...	logdecoder-t...	logdecod...	Automatic
10.17.0.1	ciscopix	ciscopix_sources	LOW	< 200 events in...	24	2015-11-10 04:29:...	1 min	2015-11-10 04:...	NWAPPLIAN...	NWAPPLI...	Manual
10.17.0.3	ciscopix	ciscopix_sources	LOW	< 200 events in...	42	2015-11-10 04:29:...	0 min	2015-11-10 04:...	NWAPPLIAN...	NWAPPLI...	Manual
10.17.0.10	ciscopix	ciscopix_sources	LOW	< 200 events in...	61	2015-11-10 04:29:...	0 min	2015-11-10 04:...	NWAPPLIAN...	NWAPPLI...	Manual
10.17.0.5	ciscopix	ciscopix_sources	LOW	< 200 events in...	107	2015-11-10 04:30:...	0 min	2015-11-10 04:...	NWAPPLIAN...	NWAPPLI...	Manual
10.17.0.7	ciscopix	ciscopix_sources	LOW	< 200 events in...	139	2015-11-10 04:30:...	0 min	2015-11-10 04:...	NWAPPLIAN...	NWAPPLI...	Manual

For procedures related to this tab, see [View Event Source Alarms](#).

Features

The Alarms tab contains the following features.

Feature	Description
Event Source	The IP, IPv6, or Hostname of the event source that is alarmed.
Event Source Type	The type of the alarmed event source. For example, winevent_nic (for Microsoft Windows) or rhlinux (for Linux).
Group	This is the event source group that contains the event source for which the alarm has been triggered.
Alarm	The type of threshold that was triggered: High or Low
Threshold Violated	The conditions of the threshold that was triggered. For example: 5,000,000 events in 5 minutes

Feature	Description
Event Count	The number of events in the threshold time period causing the alarm.
Alarmed Time	The initial time the event source went into an alarmed state. Note: When you first access this view, the data is sorted by this column (most recent alarm first).
Elapsed Time	Elapsed time since the event source entered an alarmed state.
Last Updated Time	The last time the event source was confirmed to be in an alarmed state. Note: This column is hidden by default.
Log Collector	The Log Collector last collecting from this event source.
Log Decoder	The Log Decoder last receiving from this event source.
Type	Alarm type is either Manual or Automatic : <ul style="list-style-type: none"> • Manual: these are alarms that violate the configured threshold policy. • Automatic: these are alarms that deviate from the baseline for the alarmed event source.
Filter 	Select the Filter icon to display the Filter menu: <div data-bbox="483 1318 743 1558" data-label="Image"> <p>The image shows a small window titled 'ALARM TYPE' with two checkboxes: 'Automatic' and 'Manual'. Both checkboxes are currently unchecked.</p> </div>
	Select either Automatic or Manual: <ul style="list-style-type: none"> • If you select Automatic, only the alerts that are based on baselines are displayed. • If you select Manual, only the alarms for which you have set thresholds are displayed.

Note: You can hide or show columns by right-clicking in the table header and choosing **Columns** from the drop-down menu. Select a column to display it, or clear the column to hide it.

Event Sources View

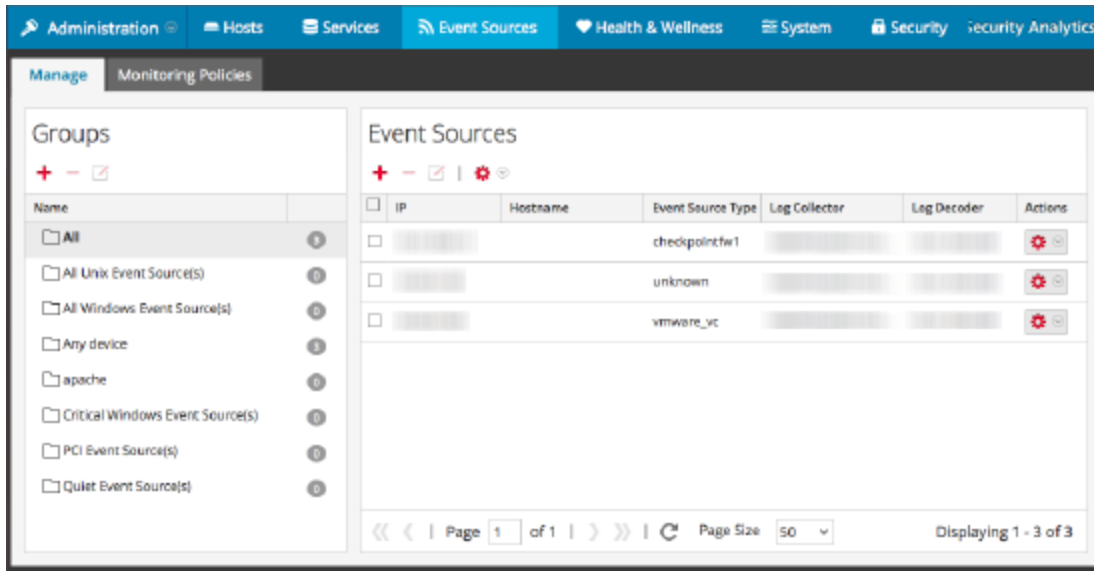
The Event Source Attributes panel has the following tabs.

Feature	Description
Manage Tab	Use this tab to create, edit, and delete Event Source Groups. It presents a customizable, searchable view of all of your event sources and groups.
Monitoring Policies Tab	Use this tab to manage alert configuration for event sources.
Alarms Tab	Use this tab to see the details of the alarms that have been generated.
Settings Tab	Use this tab to view or change the behavior for automatic (baseline) alerts.

Manage Tab

The Manage tab organizes event sources into groups, and displays attributes for each event source.

To access this tab, in the **Security Analytics** menu, select **Administration > Event Sources**. The **Manage** tab is displayed by default.

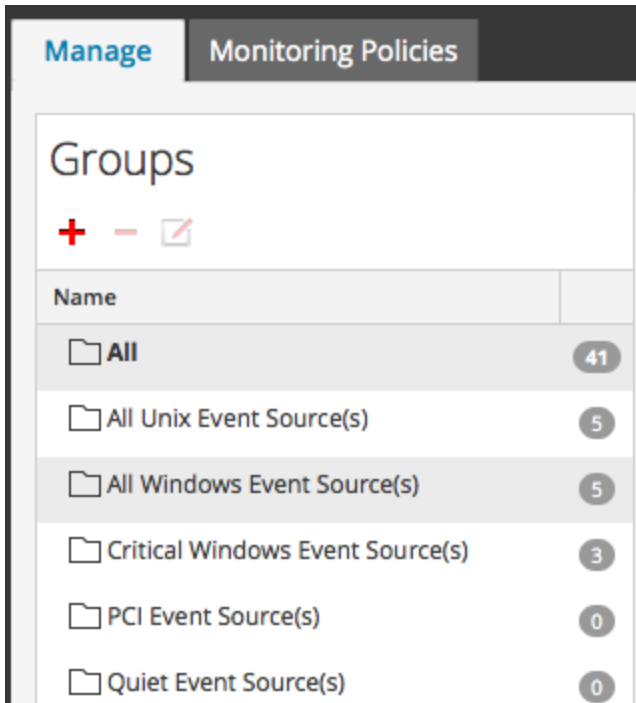


Procedures related to this tab are described in [Manage Event Source Groups](#).

The Manage tab consists of two panels, Groups and Event Sources.

Groups Panel

The Groups Panel lists the event source groups, as well as a count of the members for each group. To see all event sources, select **All** from the groups list. This is an example of the Groups panel.



The Groups panel contains the following features.

Feature	Description
Tools	These are the standard Security Analytics icons for adding, removing, or editing groups.
Count	<p>The count for an event source group indicates the number of event sources in that group. That is, the number of event sources that match the criteria used to define the group.</p> <p>Note: The count is not dynamically updated when new event sources are added. Thus, you may need to refresh to see an updated group count.</p>
Name	<p>The Name column lists the identifier for each group. You can use the group names to quickly identify some of the criteria used to form the group.</p> <p>For example, if you create a group that consists of Windows event sources for the Sales organization, you could name the group Windows Sales Sources.</p> <p>Note: The event source group name is not editable. Once you create a group, that name exists as long as the group itself.</p>

Event Sources Panel

The Event Sources panel displays the attributes for the event sources in the selected group. Or, if All is selected in the Groups panel, the Event Sources panel lists all event sources.

Event Sources


+
-
✎
⚙
▼

<input type="checkbox"/>	IP	Event Source Type	Priority	Country	Department	Actions
<input type="checkbox"/>		accurev				⚙ ▼
<input checked="" type="checkbox"/>		apache				⚙ ▼
<input type="checkbox"/>		winevent_nic				⚙ ▼
<input type="checkbox"/>		symmetrix	1			⚙ ▼
<input type="checkbox"/>		apache		US		⚙ ▼
<input type="checkbox"/>		winevent_er				⚙ ▼
<input type="checkbox"/>		MSExchangeIS ...				⚙ ▼
<input type="checkbox"/>		unknown				⚙ ▼

⏪
⏩
Page

of 1
⏪
⏩
⏲
Page Size

▼
Displaying 1 - 41 of 41

Feature	Description
Tools	<p>The toolbar contains the following tools:</p> <ul style="list-style-type: none"> • Add: manually add an event source • Remove: remove an event source • Edit: Update attributes for an existing event source • Import / Export menu,  : Displays a menu with the following options: <ul style="list-style-type: none"> • Import: Import event sources from a Content Management Database (CMDB), spreadsheet, or other tool. • Export: Export selected event sources and their attributes in CSV format. • Export Group: Export the entire group that is currently selected.
Attributes	Columnar display of attributes. You can choose which attributes to display.
Actions	Shortcut menu for often-used commands: Edit, Delete, and Export.
Check Boxes	Select rows to use when performing tasks on multiple event sources, such as bulk editing.
Navigation Tools	<p>At the bottom of the screen, there are items that help in navigating your group:</p> <ul style="list-style-type: none"> • Page <i>x</i> of <i>y</i>: indicates which page you are currently displaying, and how many total pages exist for this group. • <<, <, > and >>: click these icons to move between pages either one at a time (< and >) or to the first (<<) or last (>>) page. • Page Size: use this selector to choose your page size. • Displaying <i>x</i> - <i>y</i> of <i>z</i>: quick check of which event sources are currently displayed out of the total number for the group.

Sorting

In the Event Sources panel, the list of items is presented in a sorted order. You can choose which column on which to sort. Note, however, that the sort order depends on capitalization.

For any string column, if the values contains a mix of lower case and upper case, the upper case appear in the list before the lower case values.

For example, assume the Event Source Type column contains the following entries: Netflow, APACHE, netwitnessspectrum, ciscoasa. The sort order would be as follows:

- APACHE
- Netflow
- ciscoasa
- netwitnessspectrum

Monitoring Policies Tab

The Monitoring Policies tab organizes thresholds by event source group.

To access this tab:

1. In the **Security Analytics** menu, select **Administration > Event Sources**.
The **Manage** tab is displayed.
2. Select the **Monitoring Policies** tab.

The screenshot displays the 'Monitoring Policies' configuration page for 'PCI Event Source(s)'. The interface includes a top navigation bar and a sub-navigation bar with tabs for 'Manage', 'Monitoring Policies', 'Alarms', and 'Settings'. The 'Monitoring Policies' tab is selected.

Groups Panel:

Order ^	Group Name
1	All Unix Event Source(s)
2	All Windows Event Source(s)
3	Critical Windows Event Source(s)
4	PCI Event Source(s)
5	Quiet Event Source(s)
6	Cisco Event Sources

Monitoring Policy for PCI Event Source(s) [Save]

Enable Last Modified 2015-08-06 20:24:51

Thresholds
Define a low threshold or high threshold or both.

Low Threshold	High Threshold
< 10 events in 60 Minutes	> 1000 events in 60 Minutes

Notifications
Notify responsible parties when the alarm triggers. Choose each notification type and destination here.

+ - Notification Settings

<input type="checkbox"/>	Output	Recipient	Notification Server	Template
Click on + to add notification				

Output Suppression of every 60 minutes

Procedures related to this tab are described in [Monitor Policies](#).

The **Monitoring Policies** tab consists of three panels:

- Event Groups Panel
- Thresholds Panel
- Notifications Panel

Event Groups Panel

Groups	
Order ^	Group Name
1	All Unix Event Source(s)
2	All Windows Event Source(s)
3	Critical Windows Event Source(s)
4	PCI Event Source(s)
5	Quiet Event Source(s)
6	Cisco Event Sources

The group selected in this panel determines which thresholds appear in the Thresholds panel. You can define a set of thresholds for each event source group. Notice that the groups are listed in a specific order:

- Drag and drop groups to change the specified order.
- The higher a group is listed, the higher the precedence for that group's thresholds: RSA Security Analytics checks the thresholds in the order provided in this panel. Thus, your highest priority groups should be at the top of this list

Thresholds Panel

This is an example of the Thresholds panel for an event source group.

Monitoring Policy for **PCI Event Source(s)**

Save

Enable
Last Modified **2015-08-06 20:24:51**

Thresholds

Define a low threshold or high threshold or both.

Low Threshold	High Threshold
< 40 events in 30 Minutes	> 500 events in 30 Minutes

The Thresholds Panel contains the following features.

Feature	Description
Enable	<p>The Enable checkbox designates whether or not the thresholds that you define for a group are enabled. If so, notifications are sent whenever the thresholds for that group are outside of the defined range. If not, then no monitoring of that event source group is occurring.</p> <div data-bbox="704 537 1419 674" style="border: 1px solid green; padding: 5px;"> <p>Note: If you configure a threshold and attempt to save the page without enabling it, you receive a confirmation message, asking you whether or not to enable the policy.</p> </div> <p>If you enable a policy, but do not have any thresholds set, then you can still receive automatic (baseline) notifications, as long as you have turned on automatic notifications.</p> <p>See below for more details on the look of notifications.</p>
Low number of events Low number of minutes or hours	<p>This is the low end of the threshold. Enter the fewest number of events and the time range. If the event source group receives fewer messages than specified here, the threshold is not met, and notifications are sent.</p>
High number of events High number of minutes or hours	<p>Works similarly as for the low values: If more messages than specified here are received, the threshold is not met, and notifications are sent.</p>
Last Modified date and time	<p>This field indicates the last time and date that the thresholds were changed.</p>
Save	<p>Saves the changes you have made to the thresholds.</p>

Notifications Panel

This is an example of the Notifications panel for an event source group.

The following table describes the fields on the Notifications panel

Field	Description
Tools	The following items are available on the toolbar:
+ -	<ul style="list-style-type: none"> • Add (+): clicking the Add presents a menu where you can choose the type of the notification • Remove (-): removes the selected row from the list.
Notification Settings	Clicking this link opens a new browser tab, and takes you to the Admin > System > Notifications page in Security Analytics.
Type	Displays the type of the notification that you have chosen. The available options are as follows: <ul style="list-style-type: none"> • Email • SNMP • Syslog
Notification	See the Configure Notification Outputs topic in the <i>System Configuration Guide</i> for more details.
Notification Server	See the Configure Notification Servers topic in the <i>System Configuration Guide</i> for more details

Field	Description
Template	<p>For Event Source Management, RSA provides three out-of-the-box templates for notifications. You can use the following templates as delivered, or customize them based on the needs of your organization:</p> <ul style="list-style-type: none">• Email template: sends notifications to the specified email addresses.• SNMP template: sends notifications to the specified SNMP server• Syslog template: sends notifications to the specified Syslog server. <p>See the Configure /Templates for Notifications topic in the <i>System Configuration Guide</i> for more details.</p>
Output Sup- pression	<p>Use this item to limit how often notifications are received for this policy, in case a lot of alerts are triggered in a short period of time.</p>

The following are sample notifications, based on the supplied Templates.

- Email:

From: notifications@esm.org [mailto:notifications@esm.org]
Sent: Wednesday, November 11, 2015 11:58 AM
To:
Subject: SA-ESM Notification | High threshold triggered on PCI Event Source(s) group

RSA Security Analytics
Event Source Monitoring Notification

High threshold triggered for 10 event source(s)

Group
PCI Event Source(s)
High Threshold
Greater than 500 events in 5 minutes
Displaying 10 of 10 event sources

Source	Type	Alarm Type
10.17.0.10	ciscopix	Manual
10.17.0.13	ciscopix	Manual
10.17.0.8	ciscopix	Manual
10.17.0.8	ciscopix	Automatic
10.17.0.12	ciscopix	Manual
10.17.0.5	ciscopix	Manual
10.17.0.6	ciscopix	Manual
10.17.0.4	ciscopix	Manual
10.17.0.4	ciscopix	Automatic
10.17.0.3	ciscopix	Manual

Note: For email notifications, the third column, **Alarm Type**, specifies whether the triggered alarm was based on a user threshold, or the baseline data being out of normal bounds. If you have automatic monitoring or notifications turned off, you will not receive any **Automatic** notifications. The same is true for Syslog and SNMP, except those notifications are formatted differently.

- SNMP trap:

```
11-11-2015 11:57:33 Local7.Debug 127.0.0.1 community=public,
enterprise=1.3.6.1.4.1.36807.1.20.1, uptime=104313, agent_
ip=10.251.37.92, version=Ver2,
1.3.6.1.4.1.36807.1.20.1="Security Analytics Event Source
Monitoring Notification:
Group: PCI Event Source(s)
High Threshold:
```

Greater than 500 events in 5 minutes

10.17.0.10,ciscopix,Manual

10.17.0.13,ciscopix,Manual

10.17.0.8,ciscopix,Manual

10.17.0.8,ciscopix,Automatic

10.17.0.12,ciscopix,Manual

10.17.0.5,ciscopix,Manual

10.17.0.6,ciscopix,Manual

10.17.0.4,ciscopix,Manual

10.17.0.4,ciscopix,Automatic

10.17.0.3,ciscopix,Manual"

- Syslog sample:

```
11-11-2015 11:57:33 User.Info 127.0.0.1 Nov 11 11:57:33
localhost CEF:0|RSA|Security Analytics Event Source
Monitoring|10.6.0.0|
HighThresholdAlert|ThresholdExceeded|1|cat=PCI Event Source
(s)|Devices|
src=10.17.0.10,ciscopix,Manual|src=10.17.0.13,ciscopix,Manual|sr
c=10.17.0.8,ciscopix,Manual|src=10.17.0.8,ciscopix,Automatic|src
=10.17.0.12,ciscopix,Manual|src=10.17.0.5,ciscopix,Manual|src=10
.17.0.6,ciscopix,Manual|src=10.17.0.4,ciscopix,Manual|src=10.17.
0.4,ciscopix,Automatic|src=10.17.0.3,ciscopix,Manual|
```


Create/Edit Group Form

This Create Event Source Group form is displayed when you are creating or editing an Event Source Group.

Procedures related to this form are described in [Create Event Source Groups](#) and [Edit or Delete Event Source Groups](#).

Parameters

The following table describes the fields on the Create/Edit an Event Group form.

Field	Description
Group Name	This field is required, and appears throughout the Security Analytics UI as the identifier for the group.
Description	An optional description to help describe the purpose or details for the group.
Tools	<p>The following items are available on the toolbar:</p>  <ul style="list-style-type: none"> • Add (+): clicking the Add displays a menu where you can choose to add a condition or a group. • Remove (-): removes the selected rule or group of rules from the list. <p>When you add a new group, that has the effect of creating nested levels of conditions.</p>
Conditions	Described below, in the Rule Criteria table.
Cancel / Save	Cancel and Save options are available in the form.

Rule Criteria

The rules that you specify determine the event sources that will become part of this event source group. A rule consists of the following:

- Grouping: how the rule interacts with other rules
- Attribute: which attribute the rule is matching against
- Operator: how the rule matches the attribute
- Value: the attribute value used for the rule

The following table provides details on these rule constructors.

Rule Constructor	Details
<p>Grouping</p>	<p>You can group conditions, in order to create complex rules for an event source group. The following choices are available when grouping your rules:</p> <ul style="list-style-type: none"> • All of these: logically equivalent to AND • Any of these: logically equivalent to OR • None of these: logically equivalent to NOT <p>If you are creating a simple group, and specifying a single condition, you can leave the default value (All of these) selected.</p>
<p>Attribute</p>	<p>This contains a drop-down list, consisting of all event source attributes. The attributes are displayed by the section to which they belong. For example, all of the Identification attributes are displayed first, followed by the Properties, Importance, and so on.</p>

Rule Constructor	Details
Operator	<p>Choose from the following options:</p> <ul style="list-style-type: none"> • Equals: matches the provided value • Not equals: returns event sources whose specified attribute not equal to the provided value • In: provide a list of values in comma separated format, and event sources that match any of the provided values are included. For example: Where IP in 10.25.50.146, 10.25.50.248 This condition returns event sources that have either 10.25.50.146 or 10.25.50.248 as their IP attribute. • Not in: similar to In, except that it matches items whose attribute is not equal to any of the listed values. • Like: matches items that begin with the provided string. For example: Where Event Source Type Like Apache This condition returns event sources whose Event Source Type begins with Apache. • Not like: similar to Like, except that it matches items whose attribute does not begin with the provided string. • Greater than: matches items whose attribute is greater than the provided value. For example, if you specify Priority Greater than 5, the condition would match any item with a priority of 6 or higher. • Less than: similar to Greater than. Matches items whose attribute is less than the provided value.
Value	<p>Enter a value or group of values. The value type depends on the attribute for the condition. For example, for IPv6, you need to specify a value in IPv6 format.</p>

Settings Tab

This topic describes the features of the Settings tab. The Settings tab presents options for automatic monitoring (baseline alerting).

Note: Automatic alerting, and its settings, are currently in Beta testing.

About Automatic Alerting

You can set up policies and thresholds for your event source groups. You do this so that you receive notifications when the thresholds are not met. Security Analytics also provides an automatic way to receive alarms, if you do not want to set up thresholds to generate alarms.

To trigger automatic alerts, you can use baseline values. This way, you do not need to set up numerous group thresholds and policies in order to receive alerts. Any anomalous amount of messages trigger alerts, without needing to do any configuration (except for turning on automatic alerting).

Note the following:

- Once you begin collecting messages from an event source, it takes the system approximately a week to store a baseline value for that event source. After this initial period, the system alerts you when the number of messages for a period are above or below the baseline by a set amount. By default, this amount is 2 standard deviations above or below the baseline.
- Base your high and low deviation settings on how "regular" your event sources behave. That is, if you expect little or no variance in the number of messages that arrive for a given time (for example, 8 to 9 am on a weekday), then you can set a low value for the Deviation. Conversely, if you often see peaks and valleys, set the Deviation value higher.
- If you enable a policy, but do not have any thresholds set, then you can still receive automatic (baseline) notifications, as long as you have turned on automatic alerting.

To access this tab, in the **Security Analytics** menu, select **Administration > Event Sources > Settings**.

Automatic Monitoring Settings (Beta)

Adjust automatic event source monitoring settings and thresholds.

Monitoring Configuration

Enable Automatic Monitoring

Enable Notifications from Automatic Monitoring

Low Standard Deviations 2

High Standard Deviations 2

Enable Aggregation Persistence

Aggregation Persistence Interval in Days 120

Enable Generation of Analytics

Reset Apply

For procedures related to this tab, see [Configure Automatic Alerting](#).

Features

The Settings tab contains the following features.

Feature	Description
Enable Automatic Monitoring	Determines whether automatic alerting is on or off. By default, this option is selected (automatic alerting turned on)
Enable Notifications From Automatic Monitoring	Determines whether notifications for automatic alerts are on or off. By default, this option is cleared (automatic notifications are not sent when automatic alerts are triggered)
Low Standard Deviations	The standard deviations below which to receive alerts. Default is 2.0 (95% confidence)
High Standard Deviations	The standard deviations above which to receive alerts. Default is 2.0 (95% confidence)


Feature	Description
Enable Aggregation Persistence	<p>When selected, this option stores event source counts per one-hour interval. The data that is collected is used to form the baseline values for each event source.</p> <ul style="list-style-type: none"> • Enabled (default): one count per hour per event source is stored in the underlying database. These one-hour counts (or aggregations) form the historical basis for computing the normal range for each event source. • Disabled: when the SMS Server is restarted, Event Source Monitoring will have no historical data with which to compute the normal range and the user will have to wait until enough data (about a week's worth) is collected to form a new basis for each event source
Aggregation Persistence Interval in Days	<p>Controls how much historical data (see Enable Aggregation Persistence) to maintain for each event source. The default value of 120 days means roughly 4 months of history is kept and used when reconstructing the basis for each event source</p>
Enable Generation of Analytics	<p>When enabled, data about the behavior of the automatic alerting is stored to disk. The default value is Enabled.</p> <p>The data retained includes baseline value over time and the alerting history for each event source. Note, however, the event source address and type is anonymized, so only your event rate information is revealed.</p> <p>Since automatic alerting is a beta feature, this data is important to measure the efficacy of the feature. This can be disabled without affecting the automatic alerting functionality</p>
Reset	<p>This option discards any unsaved changes for all settings on the page</p>
Apply	<p>Click Apply to save any changes you made to the values on the page.</p>

Manage Event Source Tab

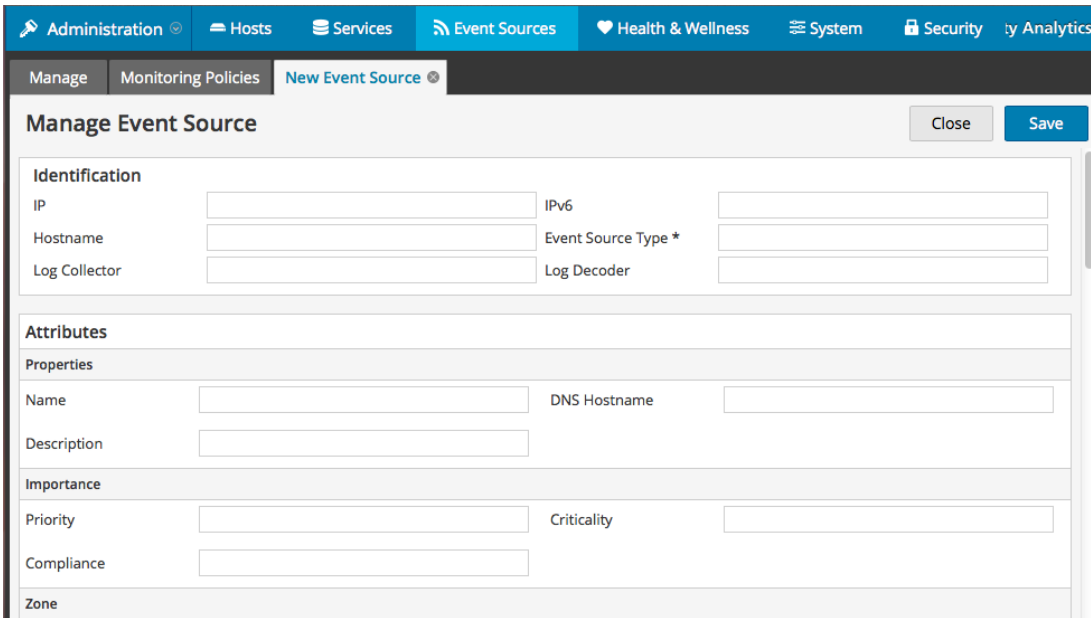
You use the Manage Event Source screen to perform the following tasks:

- Show Event Source Details
- Add attribute values to an event source
- Remove attribute values for an event source

To view the Manage Event Source screen for an event source:

1. In the **Security Analytics** menu, select **Administration > Event Sources**.
2. Select the **Manage** tab.
3. From the Event Sources pane, select an event source from the list and click + click + or .

This is an example of the New Event Source tab:



The screenshot shows the 'Manage Event Source' form with the following fields:

- Identification:** IP, Hostname, Log Collector, IPv6, Event Source Type *, Log Decoder.
- Attributes:**
 - Properties:** Name, Description, DNS Hostname.
 - Importance:** Priority, Criticality, Compliance.
 - Zone:** (field visible at the bottom)

Procedures related to this tab are described in [Create an Event Source and Edit Attributes](#).

Features

The settings in the Manage Event Source tab are a combination of auto-populated and user-entered information. When an event source sends log information to Security Analytics, it is added to the list of event sources, and some basic information is auto-populated. At any time after that, users can add or edit details for other event source attributes.

This figure shows an example of the **Identification**, **Properties**, and **Importance** sections.

Manage Event Source
Close Save

Identification

IP	<input type="text" value="192.168.1.100"/>	IPv6	F:D:D:D:D:D:D
Hostname	asd.e.dff	Event Source Type *	<input type="text" value="windows"/>
Log Collector	<input type="text" value="192.168.1.100:25565"/>	Log Decoder	INDIA_RSA_LOG_DECODER

Attributes

Properties

Name	Laptop	DNS Hostname	dnshostname
Description	This is a windows laptop		

Importance

Priority	3	Criticality	4
Compliance	4		

This figure shows an example of the **Zone**, **Location**, and **Organization** sections.

Zone			
WAN	SOME_WAN	LAN	SOME_LAN
Security	YES	Operational	YES
Location			
Country	India	State	Karnataka
County	<input type="text"/>	Province	Ring Road
City	Bangalore	Campus	India COE
Postal Code	<input type="text" value="563729"/>	Building	B Block
Floor	5	Room	C
Organization			
Company	EMC Corporation	Division	SECURITY
Business Unit	RSA	Department	RSA
Group	ASOC	Contact	ASOC Administrator
Contact Phone	0987654321	Contact EMail	asocAdmin@emc.com

Categories

This table describes the event source attribute categories.

Attribute Section	Description
Identification	<p>These attributes are the main attributes that collectively identify an event source.</p> <p>The following attributes are auto-populated, and cannot be changed while on this screen:</p> <ul style="list-style-type: none">• IP address• IPv6 value• Hostname• Event Source Type <p>These attributes can be modified:</p> <ul style="list-style-type: none">• Log Collector• Log Decoder
Properties	<p>These attributes provide the name and description.</p> <ul style="list-style-type: none">• Name• DNS Hostname• Description
Importance	<p>These attributes can be used for grouping by priority.</p> <ul style="list-style-type: none">• Priority• Criticality• Compliance
Zone	<p>These attributes can be used for grouping by zone.</p> <ul style="list-style-type: none">• WAN (Wide Area Network)• LAN (Local Area Network)• Security• Operational

Attribute Section	Description
Location	<p>These attributes can be used to group by the physical or geographical location.</p> <ul style="list-style-type: none">• Country• State• County• Province• City• Campus• Postal Code• Building• Floor• Room
Organization	<p>These attributes can be used to group by organization, and also to provide contact information.</p> <ul style="list-style-type: none">• Company• Division• Business Unit• Department• Group• Contact• Contact Phone• Contact Email
Owner	<p>These attributes specify those responsible for the event source.</p> <ul style="list-style-type: none">• Manager• Primary Administrator• Backup Administrator

Attribute Section	Description
Physical	<p>These attributes specify the physical properties for the event source.</p> <ul style="list-style-type: none">• Vendor• Serial Number• Asset Tag• Voltage• UPS Protected• Rack Height• Depth• BTU Output• Color
Function	<p>These attributes can be used to group by function.</p> <ul style="list-style-type: none">• Primary Role• Sub Role 1• Sub Role 2
System Information	<p>These attributes specify system information.</p> <ul style="list-style-type: none">• Domain Name• System Name• Identifier• System Description
Custom	<p>This section provides eight custom attributes, for any other attributes that your organization might need.</p>

Troubleshoot Event Source Management

Troubleshooting Topics:

- [Alarms and Notifications Issues](#)
- [Duplicate Log Messages](#)
- [Troubleshoot Feeds](#)
- [Import File Issues](#)
- [Negative Policy Numbering](#)

Alarms and Notifications Issues

This topic describes how to address problems you may encounter with alarms or notifications.

Alarms

If you are not seeing alarms that you expect to see, make sure that you have configured all the necessary items, as discussed below.

Automatic Alarms

To see automatic alarms appear on the Alarms screen, the **Enable Automatic Monitoring** option must be selected.

This option is on the **Setting** tab (**Administration > Event Sources > Settings**), and is selected by default. However, at some point someone may have cleared this option.

Manual Alarms

To see manual alarms appear on the Alarms screen, all of the following conditions must be met:

- The event source must be part of a Group.
- The Group must have a policy with either a low or high (or both) threshold defined.
- The Group Policy must be enabled.

Notifications

If you are seeing alarms, but are not receiving the expected notifications, make sure that you have configured all the necessary items, as discussed below.

Also, make sure that you have correctly configured the Notification Servers and Notification Outputs. Much of the preliminary configuration for Notifications is done from **Administration > System > Global Notifications**. For details, see the **Global Notifications Panel** topic in the *System Configuration Guide*.

Automatic Notifications

To have the system send automatic notifications, all of the following conditions must be met:

- The **Enable Automatic Monitoring** option must be selected (this option is selected by default).

- The **Enable Notifications From Automatic Monitoring** option must be selected. This option is cleared by default, so you or someone in your organization must select it. Navigate to **Administration > Event Sources > Settings** to see this option.
- The event source that triggered the alarm must be in a group that has a policy enabled: note that no thresholds need to be set for automatic notifications.
- The policy must at least one notification configured (either email, SNMP or Syslog).

Manual Notifications

To have the system send manual notifications (that is, a notification which says that a manual alarm was triggered):

- The event source that triggered the alarm must be in a group that has a group policy enabled.
- There must be a threshold set for the policy.
- At least one notification has been configured for the policy.

Duplicate Log Messages

It is possible that you are collecting messages from the same event source on two or more Log Collectors. This topic describes the problem and ways to troubleshoot the issue.

Details

If the ESM aggregator detects the same events for the same event source on multiple Log Collectors, you receive a warning similar to the following:


```
2015-03-17 15:25:29,221 [pool-1-thread-6] WARN
com.rsa.smc.esm.groups.events.listeners.EsmStatEventListener -
  192.0.2.21-apache had a previous event only 0 seconds ago;
likely because it exists on multiple log collectors
```

This warning message means the 192.0.2.22-apache event source is being collected by multiple hosts. You can see the list of hosts in the Log Collector column in the **Manage** tab in the Administration > Event Sources view.

Clean Up Duplicate Messages

1. Stop collectd on Security Analytics and Log Decoders:

```
Service collectd stop
```
2. Remove the ESM Aggregator persisted file on Security Analytics:

```
rm /var/lib/netwitness/collectd/ESMAggregator
```
3. Reset the Log Decoder.
 - a. Navigate to the Log Decoder REST, at `http://<LD_IP_Address>:50102`.
 - b. Click **decoder(*)** to view the properties for the decoder.
 - c. In the Properties drop-down menu, select **reset**, then click **Send**.
4. In the Event Sources panel from the Event Sources Manage tab, select all event sources and then click  to remove them.

Exporting Event Source Issues

This topic describes how to address problems you may encounter when exporting event source information.

Issue

When using a spreadsheet program to edit an exported event source CSV file, some data fields like numbers and dates can be re-formatted into the spreadsheet program's native field types. This can cause issues when re-importing this information, as some data fields may be garbled or formatted incorrectly.

Guidelines

To work around this problem, the best thing is to not open the file directly into the spreadsheet program, but rather import the text file (CSV) data into the spreadsheet program while it is already open. During the import of text data, your spreadsheet program will give you the option to have the spreadsheet program format the data as **text** so that mathematical formatting is not used on your CSV file's numbers.

Process

The exact steps differ depending on the spreadsheet program being used but the basic process is as follows:

1. Export your CSV file from Security Analytics.
You will have a CSV file on your computer. Most CSV files will open up directly into your computer's installed Spreadsheet program. However, do **not** double-click the file to open it. Instead, proceed with the following steps.
2. Open up your spreadsheet program independently.
3. Create a new workbook or blank spreadsheet in the program.
4. Look for your spreadsheet program's import functions.

Import Options

The exact method of importing into your spreadsheet is dependent upon which spreadsheet you are using. Some versions of Microsoft Excel will have an **Import Wizard** located in the **Data** menu. Other versions will have the import functions located directly in the program's main screen. Please refer to your spreadsheet program's documentation for information on importing data into the spreadsheet.

When importing the data you may be given the option to select the data type. If so, select **comma separated**. Furthermore, as part of the import you should be given the option to select the formatting that will be used for the display of the imported data.

Tip

Before selecting the format type, be sure to select all of the columns in the file, then proceed:

1. Select **text** for the format that the data will be displayed in.
2. Complete your import.

Your spreadsheet file will now be formatted in text only and preserve your numerical data as it was generated by the store.

Troubleshoot Feeds

The purpose of the feed generator is to generate a mapping of an event source to the list of groups to which it belongs.

If you have an event source from which you are collecting messages, and yet it is not displayed in the correct event source groups, then this topic provides background and information to help you track down the problem.

Details

The ESM Feed maps multiple keys to single value. It maps the DeviceAddress, Forwarder, and DeviceType attributes to groupName.

The purpose of the ESM feed is to enrich event source Meta with the groupName collected on the Log Decoder.

How it Works

The feed generator is scheduled to update every minute. However, it is triggered only if there are any changes (create, update, or delete) in event sources or groups.

It generates a single feed file with event source to group mapping, and pushes the same feed to all of the Log Decoders that are connected to Security Analytics.

Once the feed file is uploaded on the Log Decoders, for any new events, it enriches events Meta data with groupName, and appends this groupName to logstats.

Once the groupName is in logstats, the ESM Aggregator groups information and sends it to ESM. At this point, you should see the **Group Name** column under the **Event Source Monitoring** tab.

The entire process can take some time. Therefore, you may need to wait for several seconds after you add a new group or event source, before the Group name is displayed.

Note: If the event source type attribute changes when the feed is updated, Security Analytics adds a new logstats entry, rather than updating the existing one. Thus, there will be two different logstats entries in logdecoder. Previously existing messages would have been listed under the previous type, and all new messages are logged for the new event source type.

Feed File

The format of the feed file is as follows:

```
DeviceAddress, Forwarder, DeviceType, GroupName
```

The DeviceAddress is either ipv4, ipv6, or hostname, depending on which of these have been defined for the event source.

The following is a sample of the feed file:

```
"12.12.12.12", "d6", "NETFLOW", "grp1"  
"12.12.12.12", "ld4", "netflow", "grp1"  
"12.12.12.12", "d6", "netfow", "grp1"  
"0:E:507:E6:D4DB:E:59C:A", "10.25.50.243", "apache", "Apac  
hegrp"  
"1.2.3.4", "LCC", "apache", "Apachegrp"  
"10.100.33.234", "LC1", "apache", "Apachegrp"  
"10.25.50.248", "10.25.50.242", "apache", "Apachegrp"  
"10.25.50.251", "10.25.50.241", "apache", "Apachegrp"  
"10.25.50.252", "10.25.50.255", "apache", "Apachegrp"  
"10.25.50.253", "10.25.50.251", "apache", "Apachegrp"  
"10.25.50.254", "10.25.50.230", "apache", "Apachegrp"  
"10.25.50.255", "10.25.50.254", "apache", "Apachegrp"  
"13.13.13.13", "LC1", "apache", "Apachegrp"  
"AB:F255:9:8:6C88:EEC:44CE:7", , "apache", "Apachegrp"  
"Appliance1234", , "apache", "Apachegrp"  
"CB:F255:9:8:6C88:EEC:44CE:7", "10.25.50.253", "apache", "  
Apachegrp"
```

Troubleshooting Feeds

You can check the following items to narrow down where the problem is occurring.

10.5 Log Decoders

Are your Security Analytics Log Decoders at version 10.5 or later? If not, you need to upgrade them. For Security Analytics version 10.6, feeds are sent only to version 10.5 and later Log Decoders.

Feed File Existence

Verify that the feeds ZIP archive exists in the following location:

```
/opt/rsa/sms/esmfeed.zip
```

Do not modify this file.

Group Meta Populated on LD

Verify that the group meta is populated on the Log Decoder. Navigate to the Log Decoder REST and check logstats:

`http://LogDecoderIP:50102/decoder?msg=logStats&force-content-type=text/plain`

This is a sample logstats file with group information:

```
device=apache forwarder=NWAPPLIANCE10304 source=1.2.3.4
count=338 lastSeenTime=2015-Feb-04 22:30:19
lastUpdatedTime=2015-Feb-04 22:30:19
groups=IP1234Group, apacheGroup
device=apachetomcat forwarder=NWAPPLIANCE10304
source=5.6.7.8 count=1301 lastSeenTime=2015-Feb-04
22:30:19 lastUpdatedTime=2015-Feb-04 22:30:19
groups=AllOtherGroup, ApacheTomcatGroup
```

In the above text, the group information is bolded.

Device Group Meta on Concentrator

Verify that the **Device Group** meta exists on the Concentrator, and that events have values for the `device.group` field.

Device Group (8 values) 
[testgroup \(28,878\)](#) - [localgroup \(3,347\)](#) - [squid \(3,346\)](#) - [allothergroup \(780\)](#) - [apachetomcatgroup \(561\)](#) - [ip1234group \(457\)](#) - [cachefloweff \(219\)](#) - [apachegroup \(91\)](#)

sessionid	=	22133
time	=	2015-02-05T14:35:03.0
size	=	91
lc.cid	=	<input type="text" value="NWAPPLIANCE10304"/>
forward.ip	=	127.0.0.1
device.ip	=	<input type="text" value="20.20.20.20"/>
medium	=	32
device.type	=	<input type="text" value="unknown"/>
device.group	=	<input type="text" value="TestGroup"/>
kig_thread	=	"0"

SMS Log File

Check the SMS log file in the following location to view informational and error messages:
`/opt/rsa/sms/logs/sms.log`

The following are example *informational* messages:

Feed generator triggered...

Created CSV feed file.

Created zip feed file.

Pushed ESM Feed to LogDecoder : <logdecoder IP>

The following are example *error* messages:

```
Error creating CSV File : <reason>Unable to push the
ESM Feed: Unable to create feed zip archive.
Failed to add Group in CSV: GroupName: <groupName> :
Error: <error>
Unable to push the ESM Feed: CSV file is empty, make
sure you have at-least on group with at-least one
eventsources.
Unable to push the ESM Feed: No LogDecoders found.
Unable to push the ESM Feed: Unable to push feed file
on LogDecoder-<logdecoderIP>Unable to push the ESM
Feed: admin@<logdecoderIP>:50002/decoder/parsers
received error: The zip archive
"/etc/netwitness/ng/upload/<esmfeedfileName>.zip" could
not be opened
Unable to push the ESM Feed: <reason>
```

Verify Logstats data is getting Read & Published by ESMReader & ESMAggregator

These are the steps to verify that logstats are collected by **collectd** and published to Event Source Management.

ESMReader

1. On Log Decoders add **debug "true"** flag in **/etc/collectd.d/NwLogDecoder_ESM.conf**:

```
#
# Copyright (c) 2014 RSA The Security Division of EMC
#
<Plugin generic_cpp>    PluginModulePath "/usr/lib64/collectd"
    debug "true"

    <Module "NgEsmReader" "all">
        port    "56002"
        ssl     "yes"
        keypath "/var/lib/puppet/ssl/private_keys/d4c6dcd4-
6737-4838-a2f7-    ba7e9a165aae.pem"
        certpath "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-
```

```
a2f7- ba7e9a165aae.pem"
      interval "600"
      query    "all"
      <stats>
      </stats>
    </Module>
    <Module "NgEsmReader" "update">
      port      "56002"
      ssl       "yes"
      keypath   "/var/lib/puppet/ssl/private_keys/d4c6dcd4-
6737-4838-a2f7- ba7e9a165aae.pem"
      certpath  "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-
a2f7- ba7e9a165aae.pem"
      interval  "60"
      query     "update"
      <stats>
      </stats>
    </Module>
  </Plugin>
```

2. Run the command:

```
service collectd restart
```

3. Run the following command:

```
tail -f /var/log/messages | grep collectd
```

Verify that ESMReader is reading logstats and there are no errors. If there are any read issues, you will see errors similar to the following:

```
Apr 29 18:47:45 NWAPPLIANCE15788 collectd[14569]: DEBUG: NgEsmReader_
all: error getting ESM data for field "groups" from logstat
device=checkpointfw1 forwarder=PSRTEST source=1.11.51.212. Reason:
<reason>Apr 29 18:58:36 NWAPPLIANCE15788 collectd[14569]: DEBUG:
NgEsmReader_update: error getting ESM data for field "forwarder" from
logstat device=apachetomcat source=10.31.204.240. Reason: <reason>
```

ESMAggregator

1. On Security Analytics, uncomment the verbose flag in **/etc/collectd.d/ESMAggregator.conf**:

```
# ESMAggregator module collectd.conf configuration file
#
# Copyright (c) 2014 RSA The Security Division of EMC
```

```
#
<Plugin generic_cpp>
PluginModulePath "/usr/lib64/collectd"
<Module "ESMAggregator">
    verbose 1
    interval "60"
    cache_save_interval "600"
    persistence_dir "/var/lib/netwitness/collectd"
</Module>
</Plugin>
```

2. Run the following:

```
service collectd restart
```

3. Run the following command:

```
run "tail -f /var/log/messages | grep ESMA"
```

Look for ESMAggregator data and make sure your logstat entry is available in logs.

Sample output:

```
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[2] groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[4] utcLastUpdate = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator: Dis-
patching ESM stat NWAPPLIANCE15788/esma_update-cacheflowelff/esm_
counter-3.3.3.3 with a value of 1752 for NWAPPLIANCE15788/cache-
flowelff/esm_counter-3.3.3.3 aggregated from 1 log decoders
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
```

```
MetaData[2] groups = Cacheflowelfff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[4] utcLastUpdate = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator: Dis-
patching RRD stat NWAPPLIANCE15788/esma_rrd-cacheflowelfff/esm_counter-
3.3.3.3 with a value of 1752 for NWAPPLIANCE15788/cacheflowelfff/esm_
counter-3.3.3.3 aggregated from 1 log
```

Configure JMX Feed Generator Job Interval

Although the feed generation job is scheduled to execute every minute by default, you can change this by using **jconsole**, if necessary.

To change the feed generator job interval:

1. Open **jconsole** for the SMS service.
2. On the MBeans tab, navigate to **com.rsa.netwitness.sms > API > esmConfiguration > Attributes**.
3. Modify the value for the property **FeedGeneratorJobIntervalInMinutes**.
4. Go to **Operations** under the same navigation tree, and click **commit()**. This persists the new value in the corresponding json file under **/opt/rsa/sms/conf**, and uses the value if SMS is restarted.

Setting a new value reschedules the feed generator job for the new interval.

Import File Issues

If your import file is not formatted correctly, or is missing required information, an error is displayed, and the file is not imported.

Check the following:

- If you are adding unknown sources, each line in the file must contain a combination of the required attributes:
 - IP or IPv6 or Hostname, and
 - Event Source Type
- The first line of the file must contain header names, and the names must match the names in Security Analytics. To get a list of correct column names, you can export a single event source. Examine the exported CSV file: the first row of the file contains the correct set of attribute/column names.

Negative Policy Numbering

You may see negative numbers in the Order field in the Groups section of the Monitoring Policies tab. This topic describes a workaround to restore the correct numbering scheme for your policies.

Details

The following screen shows an example of the situation where the numbers of group policies become negative.

The screenshot displays the Cisco Security Analytics interface. At the top, there are navigation tabs: Administration, Hosts, Services, Event Sources, and Health & Wellness. Below these, there are sub-tabs: Manage, Monitoring Policies, and Alarms. The 'Monitoring Policies' sub-tab is active, showing a 'Monitoring Policy for Ciscoasa_Alarm14417...' configuration.

The 'Groups' section is a table with the following data:

Order ^	Group Name
-8	All Unix Event Source(s)
-8	All Windows Event So...
-8	Critical Windows Eve...
-8	PCI Event Source(s)
-8	Quiet Event Source(s)
6	Ciscoasa_Alarm14417...

The 'Monitoring Policy for Ciscoasa_Alarm14417...' configuration shows the following settings:

- Enable
- Thresholds**: Define a low threshold or high threshold or both.
 - Low Threshold: < 100 events in 5 Minutes
- Notifications**: Notify responsible parties when the alarm triggers. Choose each no...


If you encounter this situation, drag and drop the top group (**All Unix Event Source(s)**) in the above image) to after the last group (**Ciscoasa_Alarm14417**). This restores normal, ordinal numbering. You can then continue to drag and drop groups until you have them in their proper order for your organization.

Clean Up Duplicate Messages

1. Stop collectd on Security Analytics and Log Decoders:


```
Service collectd stop
```
2. Remove the ESM Aggregator persisted file on Security Analytics:

```
rm /var/lib/netwitness/collectd/ESMAggregator
```

3. Reset the Log Decoder.
 - a. Navigate to the Log Decoder REST, at `http://<LD_IP_Address>:50102`
 - b. Click **decoder(*)** to view the properties for the decoder.
 - c. In the Properties drop-down menu, select **reset**, then click **Send**.
4. In the Event Sources panel from the Event Sources Manage tab, select all event sources and then click  to remove them.