RSA NetWitness

Version 11.7

Event Sources Management

NETWITNESS

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

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

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

March 2022

Contents

NetWitness Event Sources

Event sources are network sources that send information about events to the NetWitness. They can be physical devices, such as laptops, network switches or firewall, and virtual or cloud-based applications, such as VMware. For example:

- An Apache HTTP Server
- Amazon Web Services CloudTrail
- A Barracuda Web Application Firewall
- A connection to Dropbox
- An Oracle Database
- A VMware vCenter Server

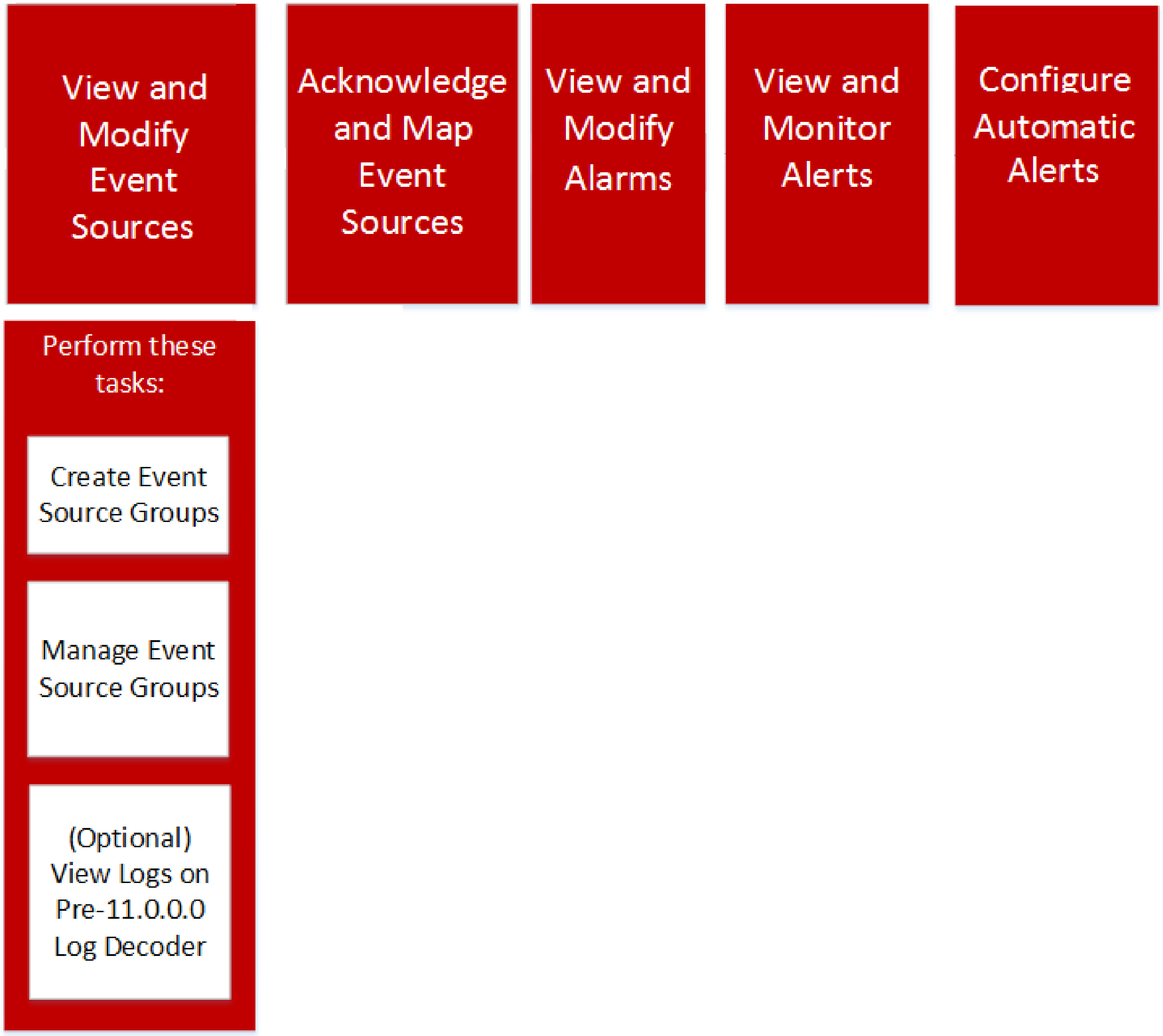
You first configure all of your event sources so that they can communicate with the NetWitness. RSA provides configuration guides for many common event sources, using a variety of collection methods (such as Syslog or file collection). After you have your event sources configured, use the information in this guide to manage them going forward.

Event Source Management

The Event Sources module in NetWitness provides an easy way to manage event sources and configure alerting policies for your event sources.

Workflow

This workflow shows the overall process for managing event sources, and configure monitoring for them. It also shows where configuring alarms and alerts settings are located in the process.


View and Modify Event Sources
Acknowledge and Map Event Sources
View and Modify Alarms
View and Monitor Alerts
Configure Automatic Alerts
Perform these tasks:
Create Event Source Groups
Manage Event Source Groups
(Optional) View Logs on Pre-11.0.0.0 Log Decoder

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 NetWitness 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 NetWitness, using roles and permissions. Available in the **System Security and User Management** guide > **Manage Users with Roles and Permissions**.

Automatic Mapping

Introduced in NetWitness version 11.1, the system maps incoming events to a type based on previous logs received from that address, reducing the mis-parsing of messages and reducing the number of items that need attention in the Discovery workflow. The User Interface (UI) indicates that an address has been auto-mapped in the Discovery workflow.

Navigate to Event Source Management

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

1. Go to 🛠 **(Admin) > Event Sources**.
2. Click any of the following:
   - The **Discovery** tab. Use this tab to review the event source types that NetWitness has discovered for each address and the system’s confidence of how likely it is that they were identified completely accurately.
   - The **Manage** tab. Use this tab to add, edit, and delete event source groups and view 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, NetWitness adds the event source to the list. Additionally, if it matches the criteria for any existing group, it becomes part of that group.

How Alarms and Notifications Work

The Event Source module in NetWitness 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**: The system sends an alert whenever an event source exceeds the thresholds in the policy for the associated groups.
- Alarms appear on the UI, in the Alarms Tab.

For notifications, consider the following:

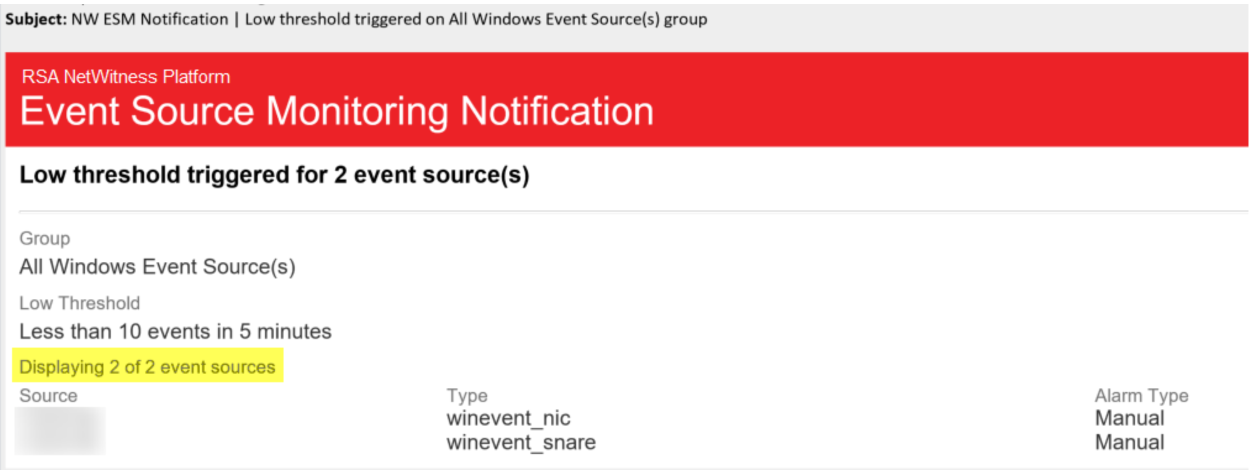
- To receive manual notifications (through email, SNMP or Syslog):
  - Specify a policy for an event source group.
  - Set a high or low (or both) threshold.
  - Enable the policy.
- To receive automatic (baseline) notifications:
  - Baseline alerting must be on. This is turned on by default.
  - You must enable notifications from automatic monitoring. See Configuring 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.

The following examples show a low threshold triggered for two event source groups and a high threshold triggered for three event source groups.



Subject: NW ESM Notification | Low threshold triggered on All Windows Event Source(s) group

RSA NetWitness Platform

Event Source Monitoring Notification

Low threshold triggered for 2 event source(s)

Group

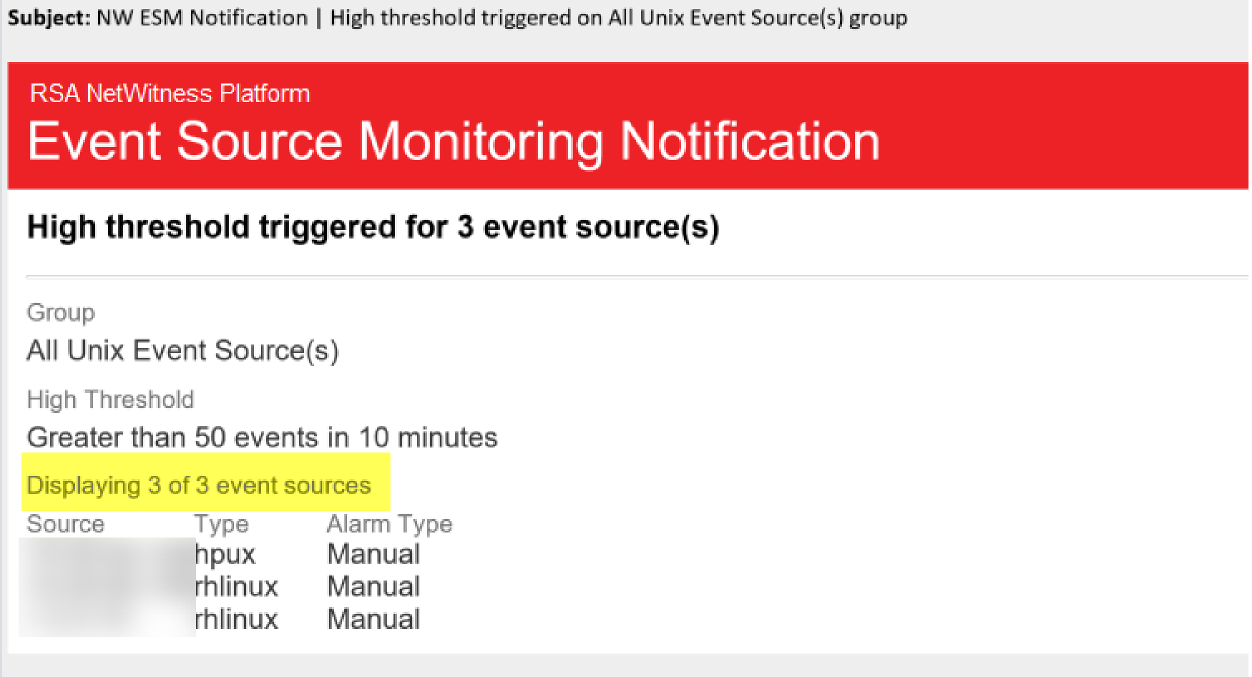
All Windows Event Source(s)

Low Threshold

Less than 10 events in 5 minutes

Displaying 2 of 2 event sources

Source	Type	Alarm Type
[redacted]	winevent_nic	Manual
	winevent_snare	Manual



Subject: NW ESM Notification | High threshold triggered on All Unix Event Source(s) group

RSA NetWitness Platform

Event Source Monitoring Notification

High threshold triggered for 3 event source(s)

Group

All Unix Event Source(s)

High Threshold

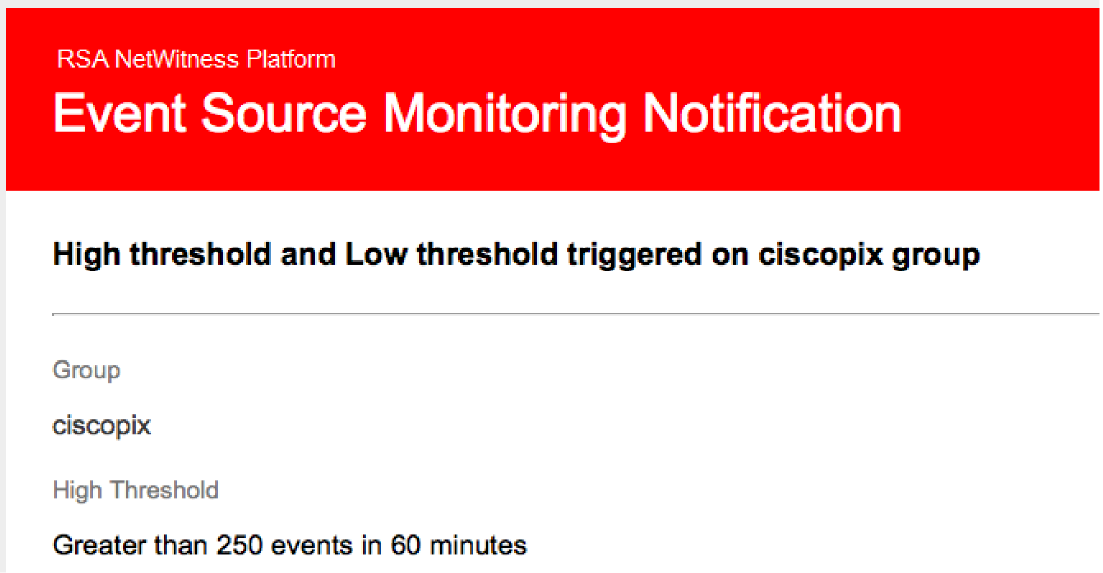
Greater than 50 events in 10 minutes

Displaying 3 of 3 event sources

Source	Type	Alarm Type
[redacted]	hpux	Manual
	rhlinux	Manual
	rhlinux	Manual

High and Low Thresholds Both Triggered

Occasionally, both the high and low alarms are 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 NetWitness Platform

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. NetWitness 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:

- After 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.)

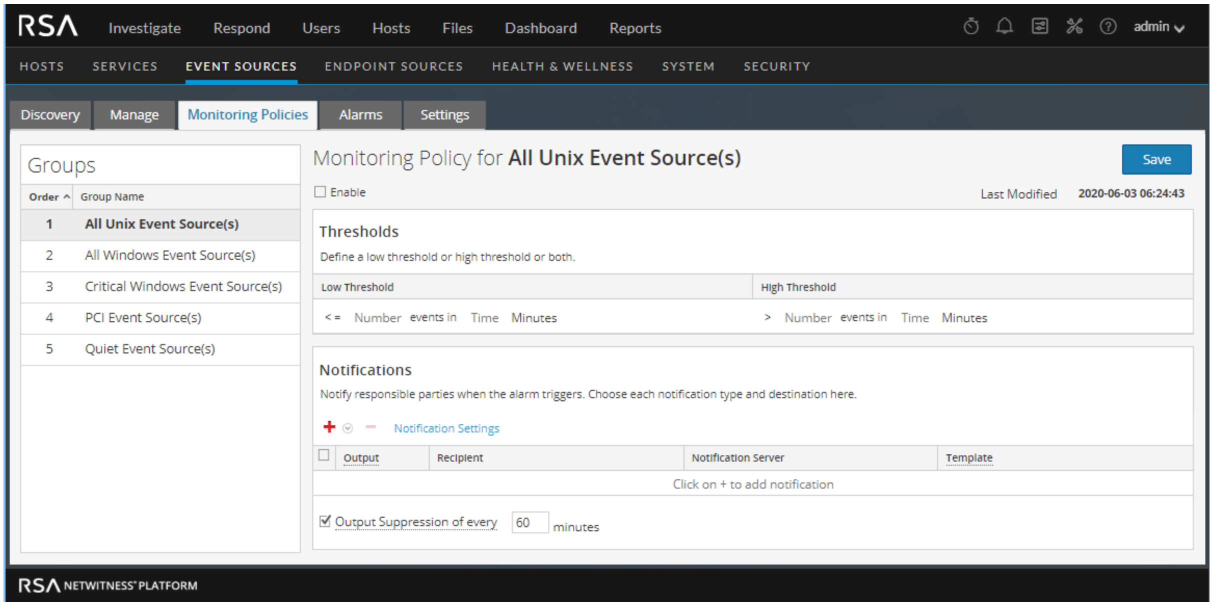
Ordering the Groups

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 NetWitness 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.
4. 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.



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)

Monitoring Policy for **All Unix Event Source(s)**

□ Enable

Last Modified 2020-06-03 06:24:43

Thresholds

Define a low threshold or high threshold or both.

Low Threshold	High Threshold
<= Number events in Time Minutes	> Number events in Time Minutes

Notifications

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

□	Output	Recipient	Notification Server	Template
Click on + to add notification				

☑ Output Suppression of every 60 minutes

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 NetWitness 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.

Managing Event Source Groups

Definitions

When dealing with event source groups in NetWitness, 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. Go to 🛠 **(Admin) > 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, NetWitness 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 NetWitness 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.

Creating Event Source Groups

Administrators must receive notifications when event sources are no longer being collected by NetWitness. 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 NetWitness 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:

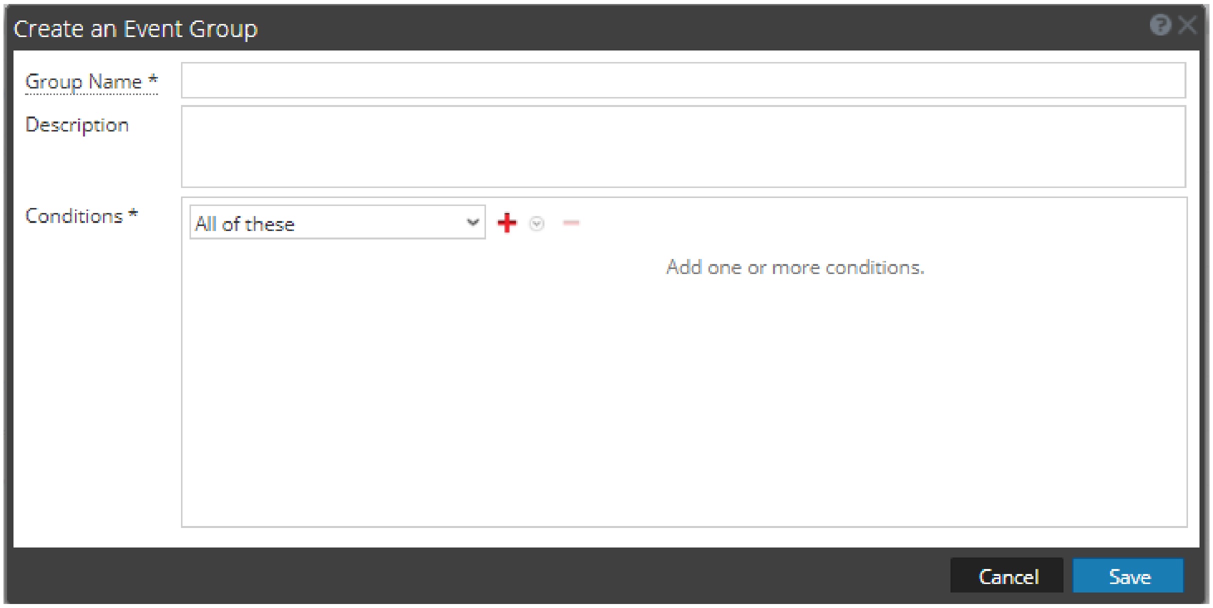
- PCI sources
- Windows Domain Controllers
- Quiet sources
- Finance Servers
- High Priority devices
- All Windows sources

Procedure

To create an Event Source group:

1. Go to 🛠 **(Admin) > Event Sources**.
2. In the **Manage** panel, click + .

   The Create an Event Group dialog is displayed.



Create an Event Group

Group Name *

Description

Conditions * All of these

Add one or more conditions.

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.

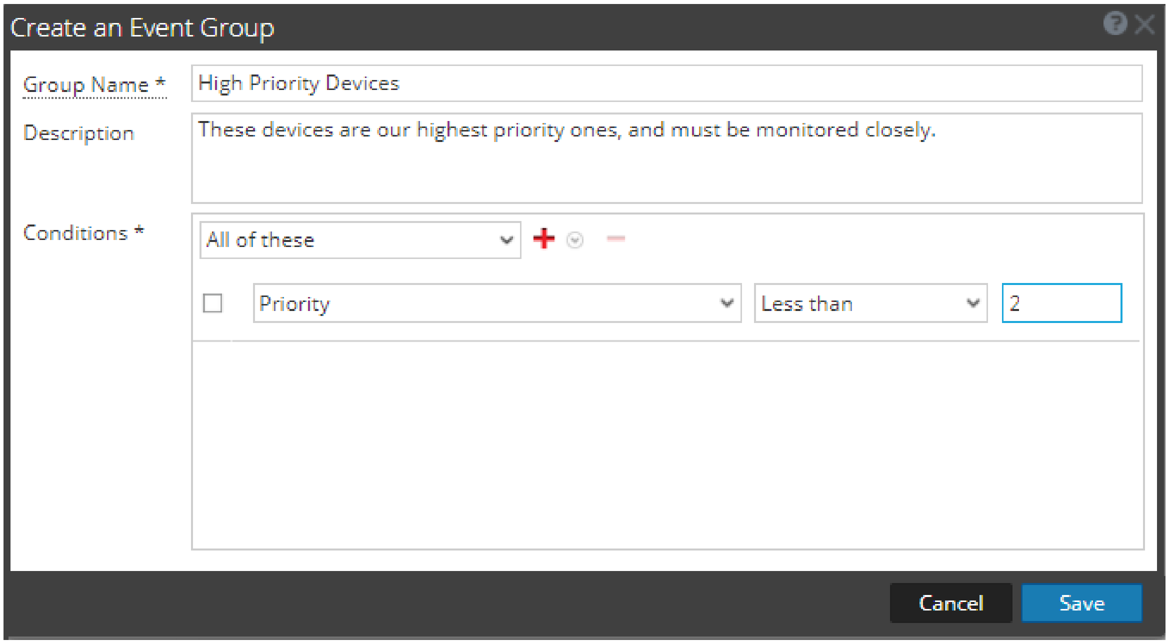
1. Go to **(Admin) > Event Sources**.
2. In the **Manage > Groups** panel, click + .
3. Enter **High Priority Devices** for the Group Name.
4. Enter a description, such as, "These devices are our highest priority ones, and must be monitored closely."
5. Leave **All of these** selected and click + to 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.



Create an Event Group

Group Name * High Priority Devices

Description These devices are our highest priority ones, and must be monitored closely.

Conditions * All of these

□ Priority Less than 2

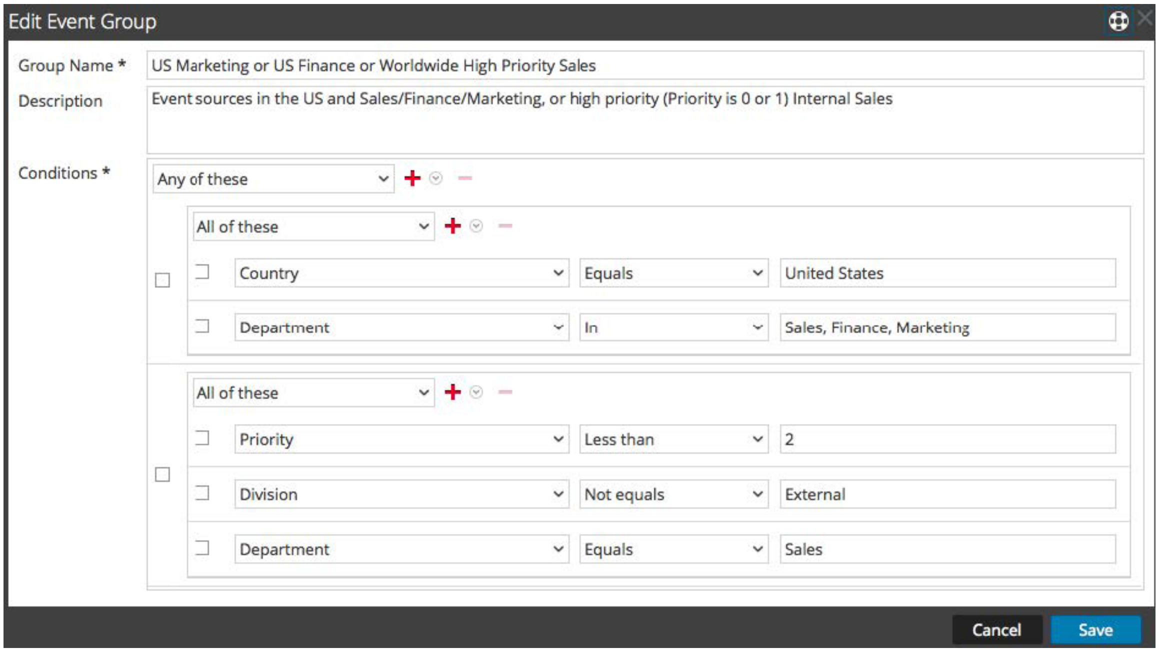
7. Click **Save**.

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.



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 Equals United States
  - □ Department In Sales, Finance, Marketing
- □ All of these
  - □ Priority Less than 2
  - □ Division Not equals External
  - □ Department Equals Sales

Creating Event Source Group Form

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

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 NetWitness UI as the identifier for the group.
Description	An optional description to help describe the purpose or details for the group.
Tools + ⊙ −	The following items are available on the toolbar: • **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. When you add a new group, that has the effect of creating nested levels of conditions.
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
Grouping	You can group conditions, in order to create complex rules for an event source group. The following choices are available when grouping your rules: • **All of these**: logically equivalent to AND • **Any of these**: logically equivalent to OR • **None of these**: logically equivalent to NOT If you are creating a simple group, and specifying a single condition, you can leave the default value (**All of these**) selected.
Attribute	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.

Rule Constructor	Details

Operator	Choose from the following options:
	• **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	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.

Acknowledging and Mapping Event Sources

In NetWitness version 11.1, RSA introduced Automatic Mapping. The system automatically maps incoming events to a type based on previous logs received from that address, reducing the number of items that need attention in the Discovery workflow. The UI indicates that an address has been auto-mapped in the Discovery workflow.

Acknowledge Event Source Types

The Discovery tab lets you review the event source types that NetWitness has discovered for each address and the system’s confidence of how likely it is that they were identified accurately. If the discovered event source types are correct, you can acknowledge to filter out that event source from the view by default. If incorrect, you can set the allowed event source types for a particular address so that future logs will parse against the correct parsers.

To acknowledge event sources:

1. Go to **(Admin) > Event Sources**.

   The Discovery tab is displayed.

2. Select one or more event sources.
3. Click **Toggle Acknowledge**.

Note the following:

- After Event Sources are Acknowledged, they are no longer displayed in the Event Source Type(s) column.
- The **Toggle Acknowledge** button behaves as follows:
  - If the Acknowledged state for all of the selected event sources is the same, all values are toggled. That is, if you select only event sources with **Yes** in Acknowledged column, the value changes to **No** for all of them. Similarly if they all have **No** in the Acknowledged column, the value changes to **Yes** for all selected event sources.
  - If you select a multiple event sources, and the value for some is **Yes** and for other it is **No**, when you click **Toggle Acknowledge**, all of the values are set to **Yes** for the selected event sources.

Note: Acknowledged Event Sources are not displayed by default.

Manually Map Event Source Types

When discovered event source types are not completely accurate, you can manually map the parsers to obtain additional information.

To map one or more event sources:

1. Go to **(Admin) > Event Sources**.

   The Discovery tab is displayed.

2. Select one or more event sources.
3. Click Map .

   The Manage Parser Mappings dialog box is displayed.

> **Note:** For event sources that were created manually, the Manage Parser Mappings window has an empty Display Name in the Log Parsers column. To view the missing display names, close the Manage Parser Mappings dialog box, and then reopen it.

4. Add or remove parser mappings, and change the priority order, based on the needs of your organization. For more details, see Manage Parser Mappings .

> **Note:** Discovery scores for the mapped Event Sources are listed in the Event Source Type(s) column from the lowest to highest discovery scores. Discovery scores range from 0 (least confident) to 100 (most confident).

Viewing Logs from Pre-11.0 Log Decoder

NetWitness 11.0 added the capability to view a small sampling of recent logs for specific devices through detail tabs of the Discovery View. By default, Log Decoders prior to 11.0 do not have the necessary configuration to enable this feature, but a few minor changes can make it available. For more details, see Viewing Logs from Pre-11.0 Log Decoder.

Editing or Deleting 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 NetWitness.

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. After you create a group, that name exists as long as the group itself exists.

Edit an Event Source Group

1. Go to 🛠 **(Admin) > 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. Go to 🛠 **(Admin)** > **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.

Removing Idle Event Sources

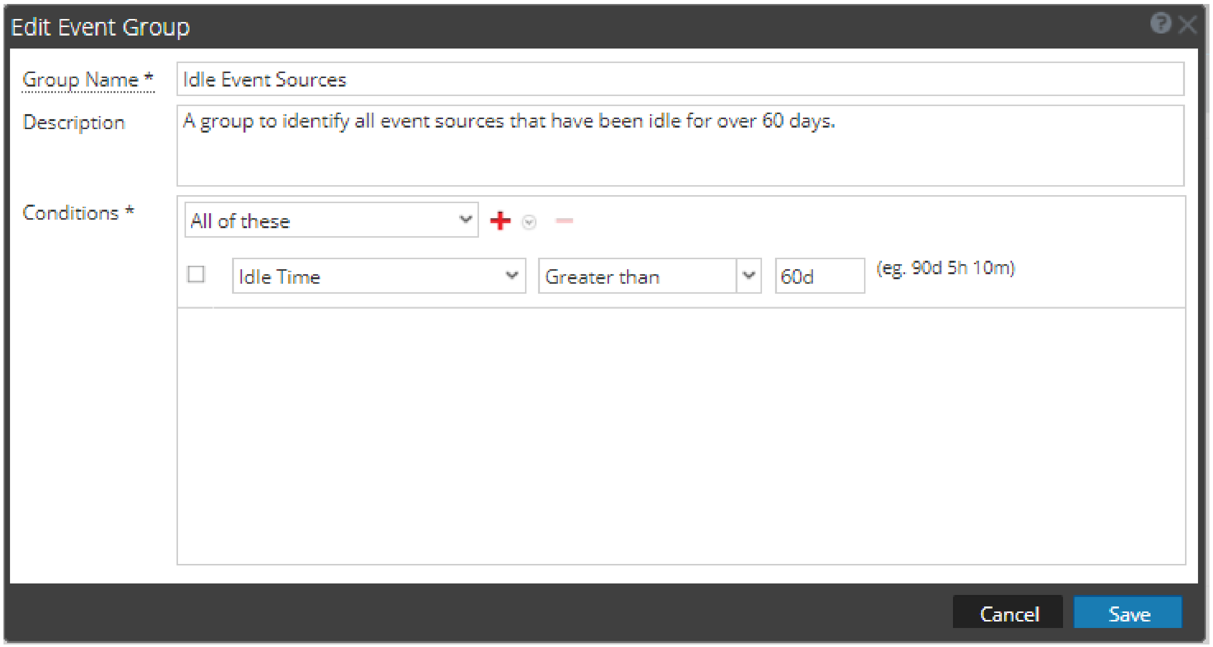
Periodically, you may want to update your set of event sources, and remove ones that are no longer being used. You can use the **Idle Time** parameter to do this.

Note: The information in this topic applies to NetWitness Version 11.2 and later.

To remove idle event sources:

1. Go to 🛠 **(Admin)** > **Event Sources**.
2. In the **Manage** panel, click + .

   The Create an Event Group dialog is displayed.
3. Fill in the name and description as you like, and add a condition that uses the **Idle Time** parameter, as shown here:



Edit Event Group

Group Name * Idle Event Sources

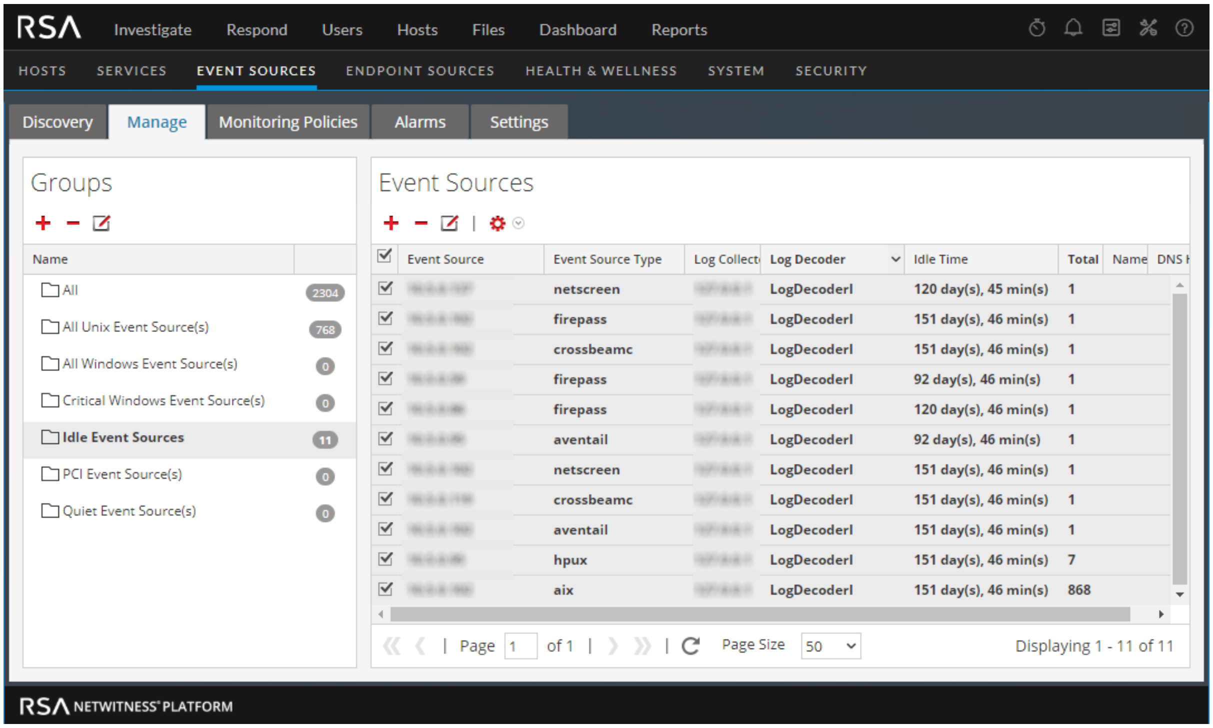
Description A group to identify all event sources that have been idle for over 60 days.

Conditions * All of these

□ Idle Time | Greater than | 60d (eg. 90d 5h 10m)

In this example, we have set the condition to identify event sources that have been idle for at least 60 days.

4. Save the new group, then select it in the Groups panel.
5. Select some or all event sources in the group. The following screen shows all event sources from this group selected.



Groups

Name	
All	2304
All Unix Event Source(s)	768
All Windows Event Source(s)	0
Critical Windows Event Source(s)	0
Idle Event Sources	11
PCI Event Source(s)	0
Quiet Event Source(s)	0

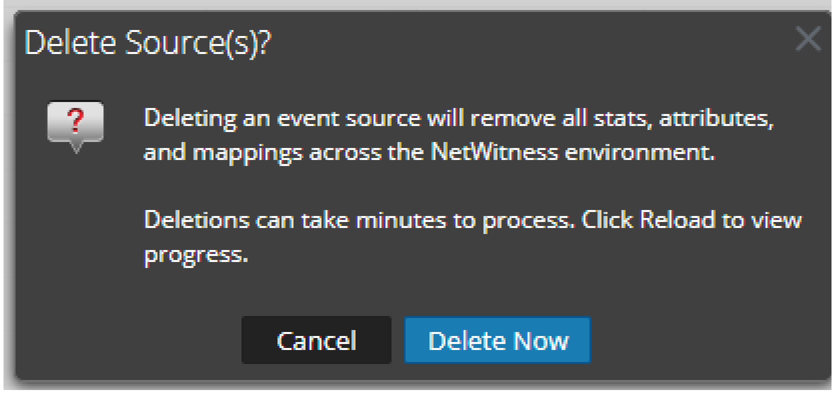
Event Sources

☑	Event Source	Event Source Type	Log Collect	Log Decoder	Idle Time	Total	Name	DNS H
☑	[redacted]	netscreen	[redacted]	LogDecoderI	120 day(s), 45 min(s)	1		
☑	[redacted]	firepass	[redacted]	LogDecoderI	151 day(s), 46 min(s)	1		
☑	[redacted]	crossbeamc	[redacted]	LogDecoderI	151 day(s), 46 min(s)	1		
☑	[redacted]	firepass	[redacted]	LogDecoderI	92 day(s), 46 min(s)	1		
☑	[redacted]	firepass	[redacted]	LogDecoderI	120 day(s), 46 min(s)	1		
☑	[redacted]	aventail	[redacted]	LogDecoderI	92 day(s), 46 min(s)	1		
☑	[redacted]	netscreen	[redacted]	LogDecoderI	151 day(s), 46 min(s)	1		
☑	[redacted]	crossbeamc	[redacted]	LogDecoderI	151 day(s), 46 min(s)	1		
☑	[redacted]	aventail	[redacted]	LogDecoderI	151 day(s), 46 min(s)	1		
☑	[redacted]	hpux	[redacted]	LogDecoderI	151 day(s), 46 min(s)	7		
☑	[redacted]	aix	[redacted]	LogDecoderI	151 day(s), 46 min(s)	868		

Page 1 of 1 | Page Size 50 | Displaying 1 - 11 of 11

6. In the Event Sources panel, click − to delete the selected, idle event sources.

A confirmation message appears:



Delete Source(s)?

Deleting an event source will remove all stats, attributes, and mappings across the NetWitness environment.

Deletions can take minutes to process. Click Reload to view progress.

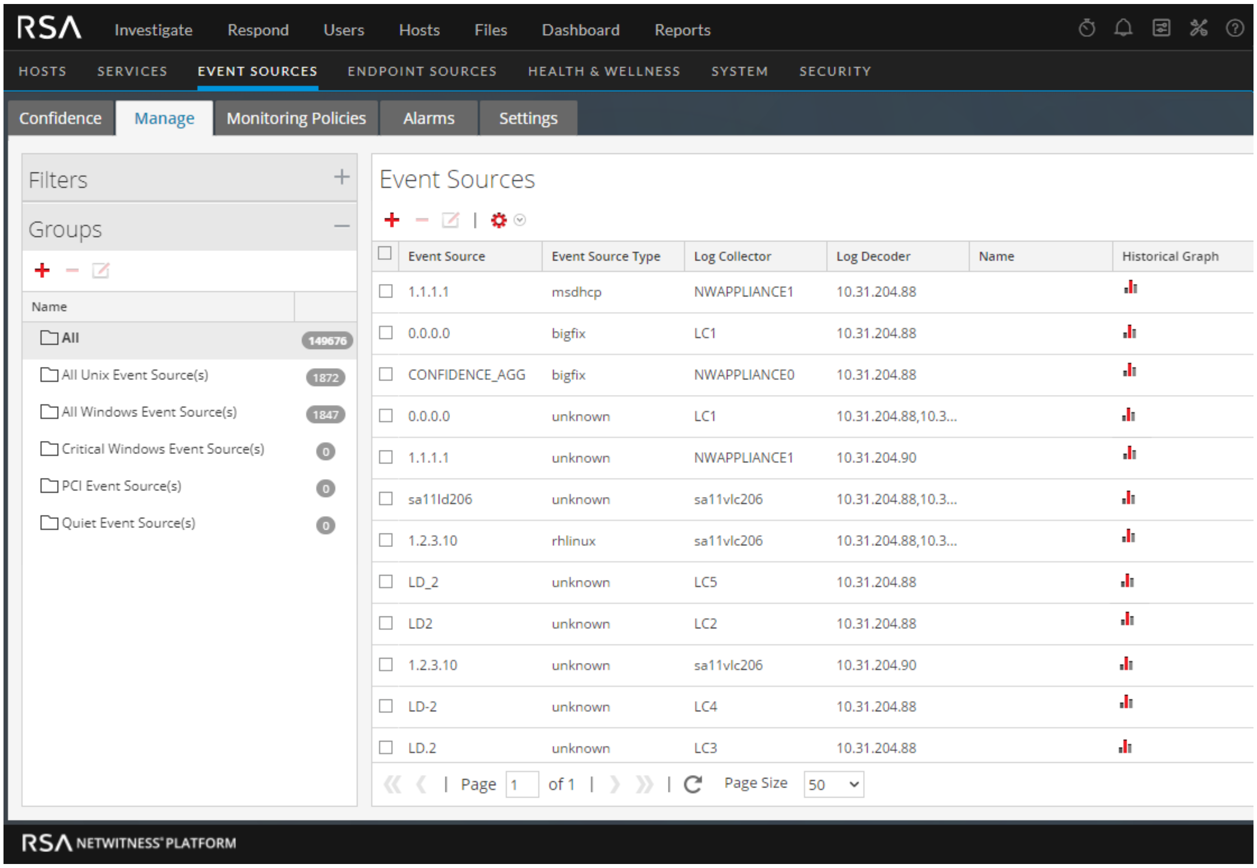
7. Click Delete Now to confirm your intention to delete the selected event sources.

If, in the future, an event source that has been removed sends logs, a new event source will be created.

Creating an Event Source and Editing 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:



Name	
All	149676
All Unix Event Source(s)	1872
All Windows Event Source(s)	1847
Critical Windows Event Source(s)	0
PCI Event Source(s)	0
Quiet Event Source(s)	0

Event Source	Event Source Type	Log Collector	Log Decoder	Name	Historical Graph
1.1.1.1	msdhcp	NWAPPLIANCE1	10.31.204.88		
0.0.0.0	bigfix	LC1	10.31.204.88		
CONFIDENCE_AGG	bigfix	NWAPPLIANCE0	10.31.204.88		
0.0.0.0	unknown	LC1	10.31.204.88,10.3...		
1.1.1.1	unknown	NWAPPLIANCE1	10.31.204.90		
sa11ld206	unknown	sa11vlc206	10.31.204.88,10.3...		
1.2.3.10	rhlinux	sa11vlc206	10.31.204.88,10.3...		
LD_2	unknown	LC5	10.31.204.88		
LD2	unknown	LC2	10.31.204.88		
1.2.3.10	unknown	sa11vlc206	10.31.204.90		
LD-2	unknown	LC4	10.31.204.88		
LD.2	unknown	LC3	10.31.204.88		

Event source attributes are a combination of auto-populated and user-entered information. When an event source sends log information to NetWitness, 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. After 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 NetWitness 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. Go to **(Admin) > 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**.

Note: The Discovery Score is listed as **Unavailable** for manually-added event sources. The score remains as **Unavailable** until the event source begins sending information to the NetWitness

Update Attributes for an Event Source

1. Go to **(Admin) > 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 after you have entered them.
6. Click **Save**

Bulk Editing 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.

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

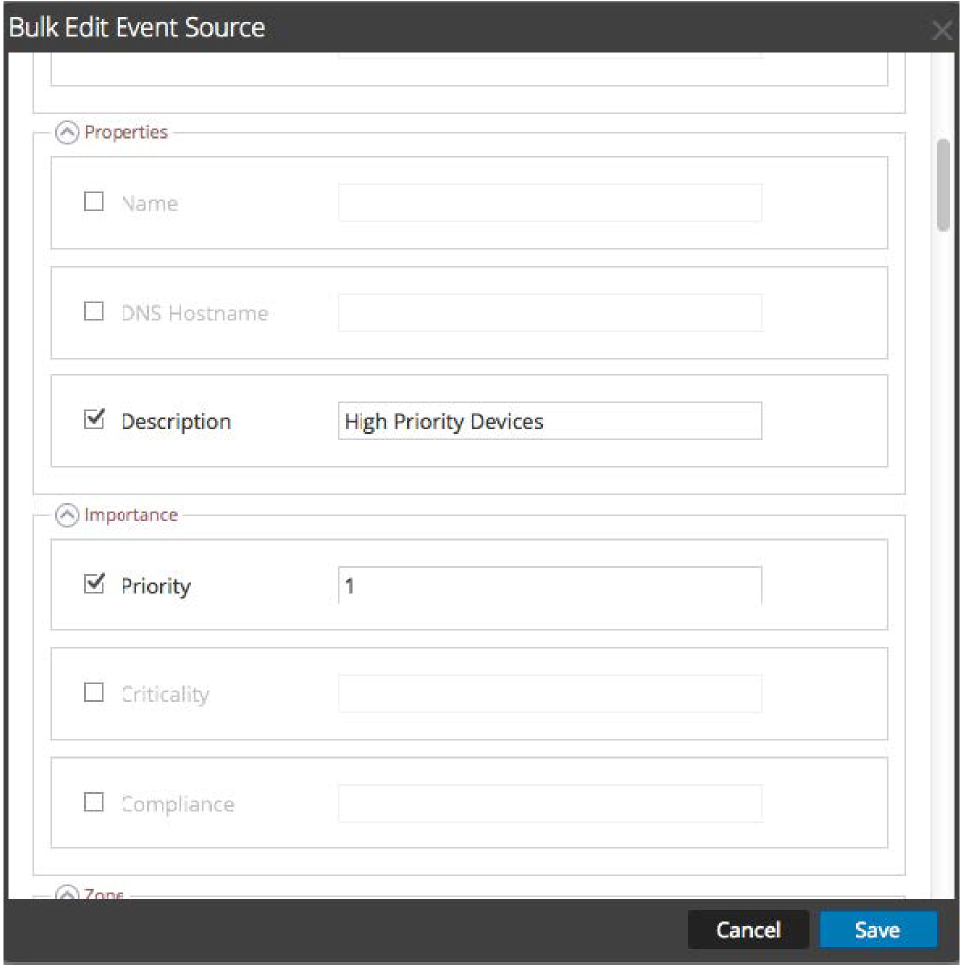
To bulk edit attributes for Event Sources:

1. Go to **(Admin) > 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.



Bulk Edit Event Source

Properties

- □ Name
- □ DNS Hostname
- ☑ Description: High Priority Devices

Importance

- ☑ Priority: 1
- □ Criticality
- □ Compliance

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**.

Importing 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 NetWitness), the original value in NetWitness 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 NetWitness 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 NetWitness, the attributes for that event source are ignored. That is, NetWitness does **not** create a new event source for these attributes.
- If the event source exists in both the import file and NetWitness, values for that event source are overwritten.
- If an attribute is blank in the import file, it clears the corresponding attribute in NetWitness.
- If an attribute is not specified in the import file, then the corresponding attribute is ignored in NetWitness (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 NetWitness 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.

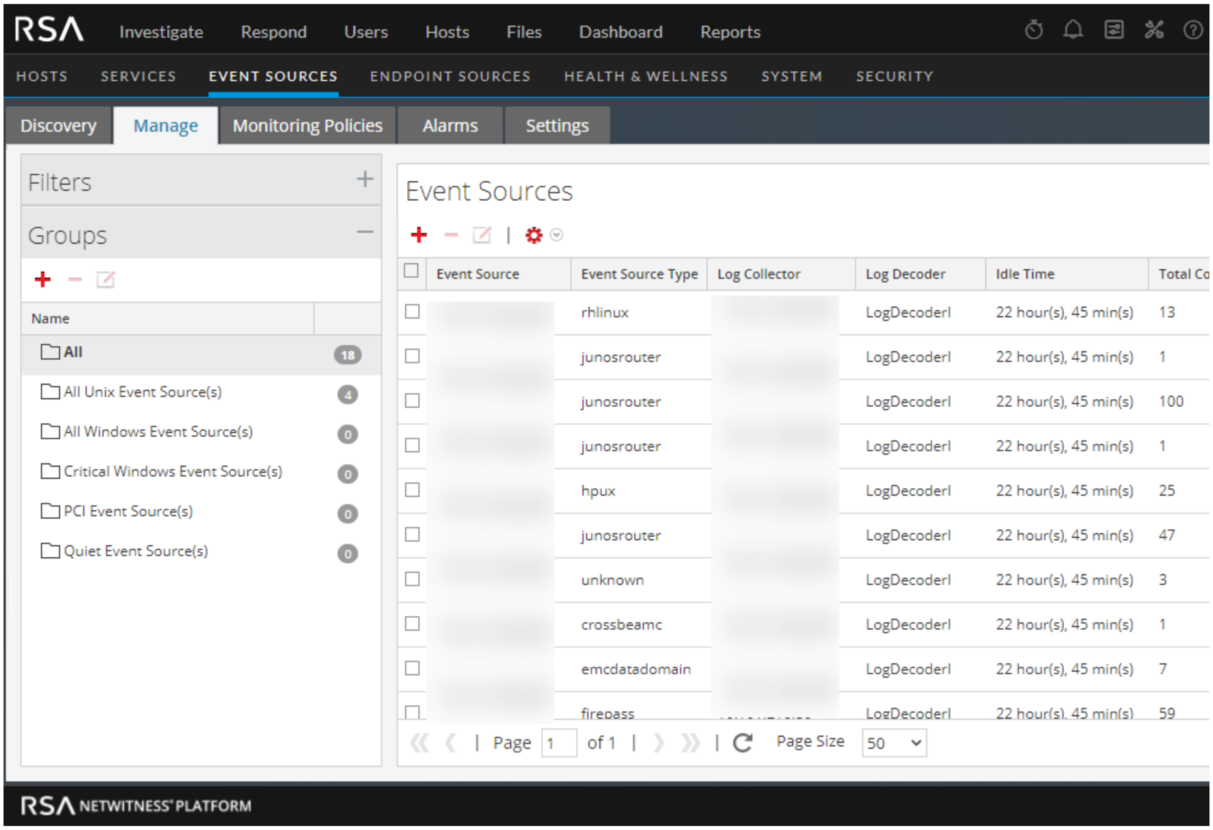
The above behaviors are the defaults—you can change the behavior as specified in the following procedure.

Import Event Source Attributes

To import Event Source attributes from a file:

1. Go to 🛠 **(Admin) > Event Sources**.
2. Select the **Manage** tab.

   The Event Sources Manage tab is displayed.

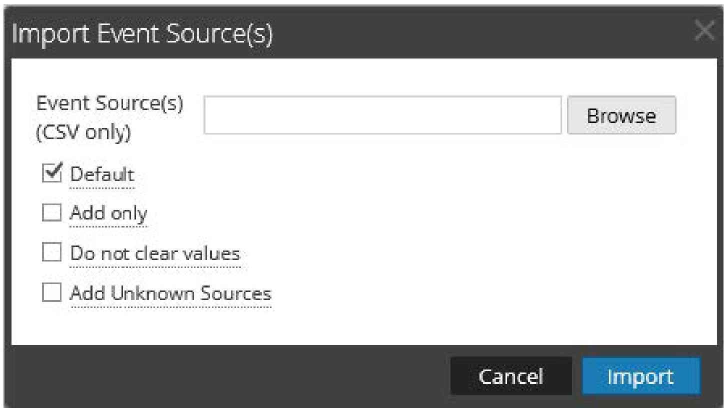


Name	
All	18
All Unix Event Source(s)	4
All Windows Event Source(s)	0
Critical Windows Event Source(s)	0
PCI Event Source(s)	0
Quiet Event Source(s)	0

☐	Event Source	Event Source Type	Log Collector	Log Decoder	Idle Time	Total Co
☐	[redacted]	rhlinux	[redacted]	LogDecoderI	22 hour(s), 45 min(s)	13
☐	[redacted]	junosrouter	[redacted]	LogDecoderI	22 hour(s), 45 min(s)	1
☐	[redacted]	junosrouter	[redacted]	LogDecoderI	22 hour(s), 45 min(s)	100
☐	[redacted]	junosrouter	[redacted]	LogDecoderI	22 hour(s), 45 min(s)	1
☐	[redacted]	hpux	[redacted]	LogDecoderI	22 hour(s), 45 min(s)	25
☐	[redacted]	junosrouter	[redacted]	LogDecoderI	22 hour(s), 45 min(s)	47
☐	[redacted]	unknown	[redacted]	LogDecoderI	22 hour(s), 45 min(s)	3
☐	[redacted]	crossbeamc	[redacted]	LogDecoderI	22 hour(s), 45 min(s)	1
☐	[redacted]	emcdatadomain	[redacted]	LogDecoderI	22 hour(s), 45 min(s)	7
☐	[redacted]	firepass	[redacted]	LogDecoderI	22 hour(s), 45 min(s)	59

3. From the Import/Export menu in the toolbar (⚙), select **Import** (Import).

   The Import Event Sources dialog is displayed.



Event Source(s) (CSV only)

☑ Default

☐ Add only

☐ Do not clear values

☐ Add Unknown Sources

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 NetWitness is blank. Thus, no existing values will be overwritten.

- **Do not clear values**: Does not clear attribute values in NetWitness 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 NetWitness. 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.

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

Exporting Event Sources

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

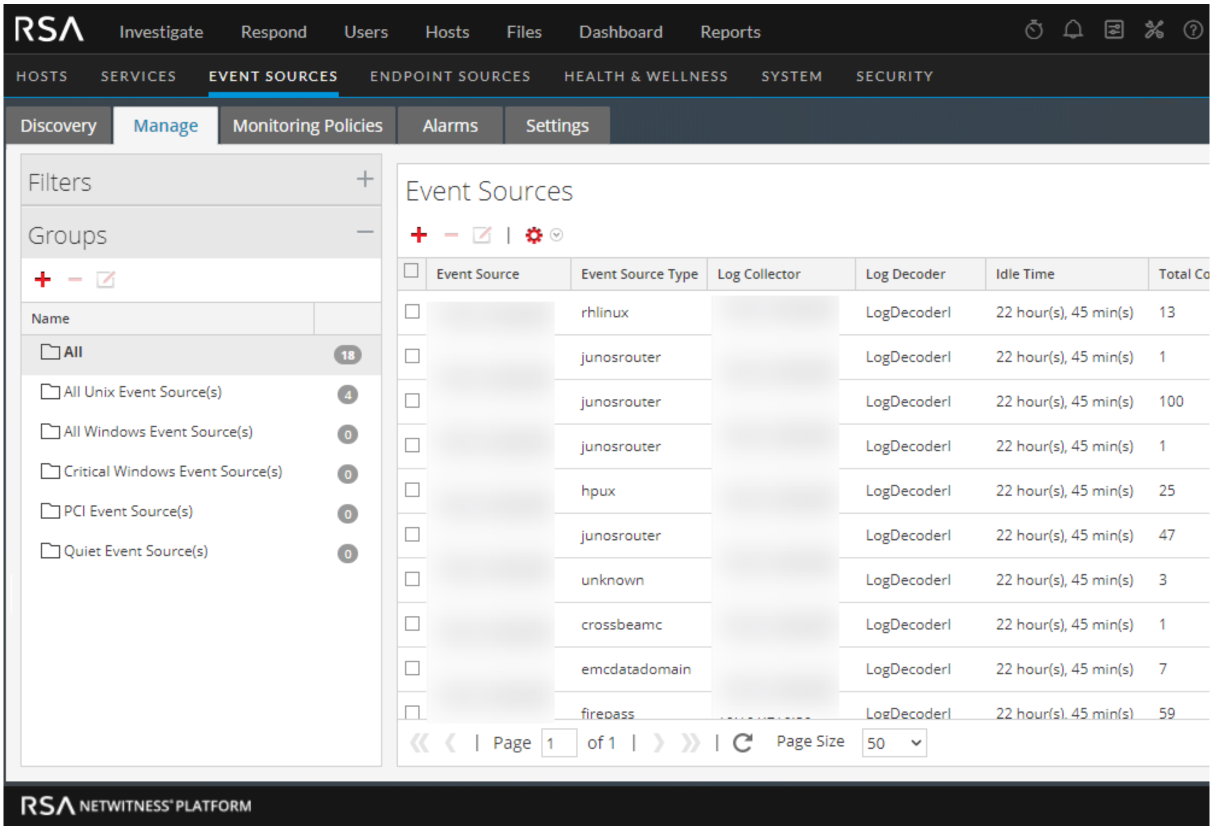
Note the following:

- 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.

To export your Event Sources:

1. Go to **(Admin) > Event Sources**.
2. Select the **Manage** tab.

   The Event Sources Manage tab is displayed.

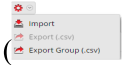


Name	
All	18
All Unix Event Source(s)	4
All Windows Event Source(s)	0
Critical Windows Event Source(s)	0
PCI Event Source(s)	0
Quiet Event Source(s)	0

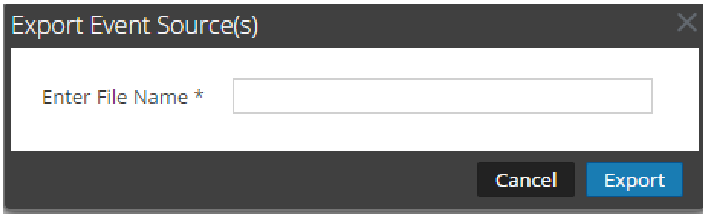
□	Event Source	Event Source Type	Log Collector	Log Decoder	Idle Time	Total Co
□	[redacted]	rhlinux	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	13
□	[redacted]	junosrouter	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	1
□	[redacted]	junosrouter	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	100
□	[redacted]	junosrouter	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	1
□	[redacted]	hpux	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	25
□	[redacted]	junosrouter	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	47
□	[redacted]	unknown	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	3
□	[redacted]	crossbeamc	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	1
□	[redacted]	emcdatadomain	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	7
□	[redacted]	firepass	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	59

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**.

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

Sorting Event Sources

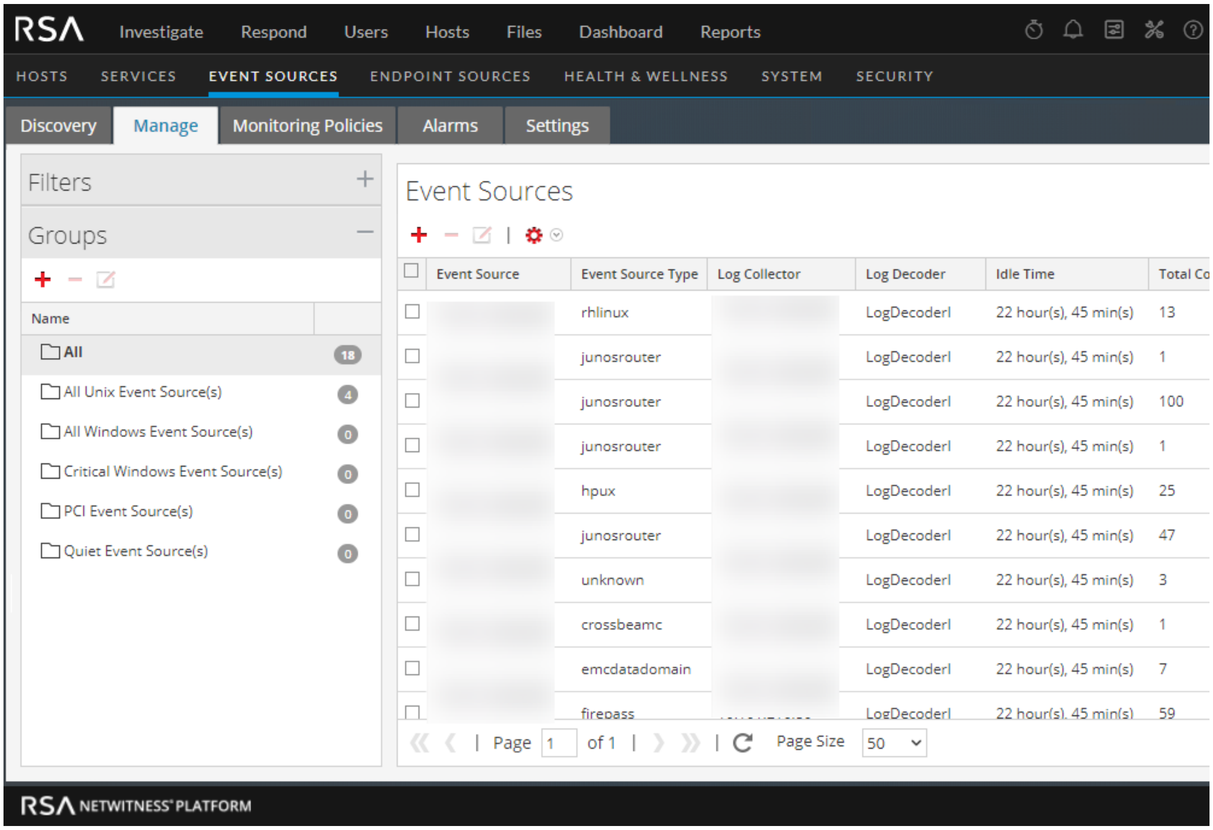
The event sources panel displays attributes for the currently selected event source group. You can configure the list of attributes that are displayed, as well as sort the list on any of the displayed attributes.

Note: The 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.)

To sort your event sources:

1. Go to **(Admin) > Event Sources**.
2. Select the **Manage** tab.

   The Event Sources Manage tab is displayed.



Name	
All	18
All Unix Event Source(s)	4
All Windows Event Source(s)	0
Critical Windows Event Source(s)	0
PCI Event Source(s)	0
Quiet Event Source(s)	0

□	Event Source	Event Source Type	Log Collector	Log Decoder	Idle Time	Total Co
□	[redacted]	rhlinux	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	13
□	[redacted]	junosrouter	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	1
□	[redacted]	junosrouter	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	100
□	[redacted]	junosrouter	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	1
□	[redacted]	hpux	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	25
□	[redacted]	junosrouter	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	47
□	[redacted]	unknown	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	3
□	[redacted]	crossbeamc	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	1
□	[redacted]	emcdatadomain	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	7
□	[redacted]	firepass	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	59

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.

Monitoring 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 Configuring Automatic Alerting to view alarms when the number of messages for an event source are outside of the normal bounds.

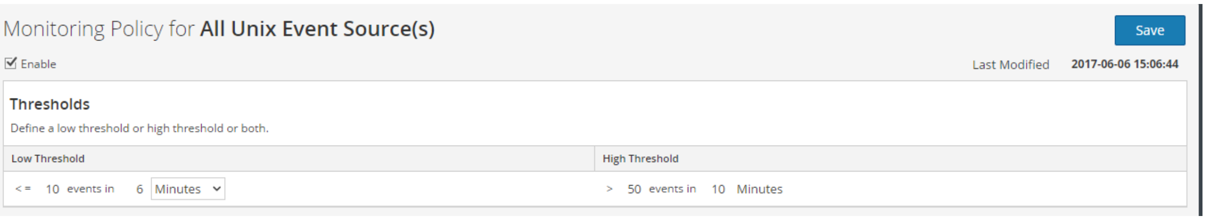
Configuring Event Source Group Alerts

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. Go to **(Admin) > 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 **All Unix Event Source(s)**

☑ Enable

Last Modified **2017-06-06 15:06:44**

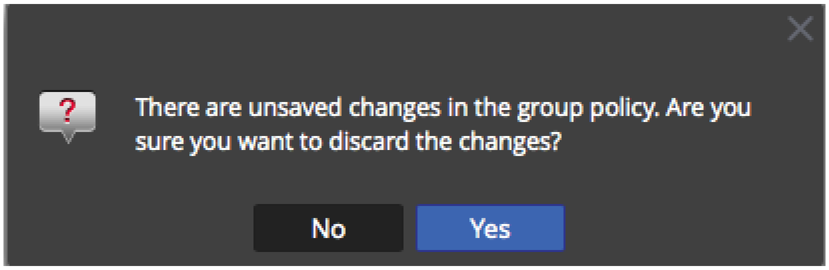
Thresholds

Define a low threshold or high threshold or both.

Low Threshold	High Threshold
<= 10 events in 6 Minutes	> 50 events in 10 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:



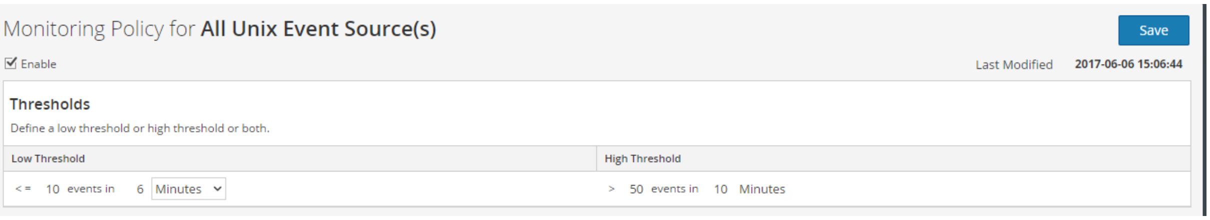
There are unsaved changes in the group policy. Are you sure you want to discard the changes?

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.

If you configure longer policy duration for low threshold policy, it may result in increased memory (SMS Heap) usage. In order to avoid increased memory usage (For more information, see 'Troubleshooting Health & Wellness' in the *System Maintenance Guide*), make sure you optimize the policy filter to match the required Event Sources and also RSA recommends having a policy duration of < 3 days if 30 low threshold policies match 20K Event Sources. If there are < 10 low threshold policies, you can have < 7 days policy duration with each policy matching unique Event Sources.

1. Go to **(Admin) > 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 **All Unix Event Source(s)**

☑ Enable

Last Modified **2017-06-06 15:06:44**

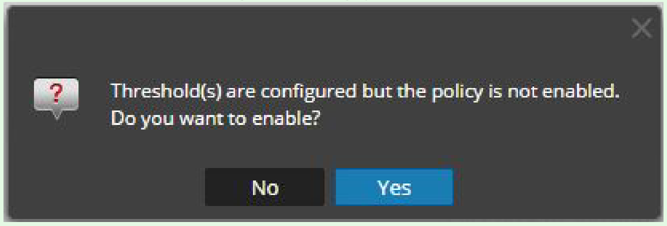
Thresholds

Define a low threshold or high threshold or both.

Low Threshold	High Threshold
<= 10 events in 6 Minutes	> 50 events in 10 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.
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: ddd



Threshold(s) are configured but the policy is not enabled. Do you want to enable?

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.

After 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.

Setting 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. Go to (Admin) > **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

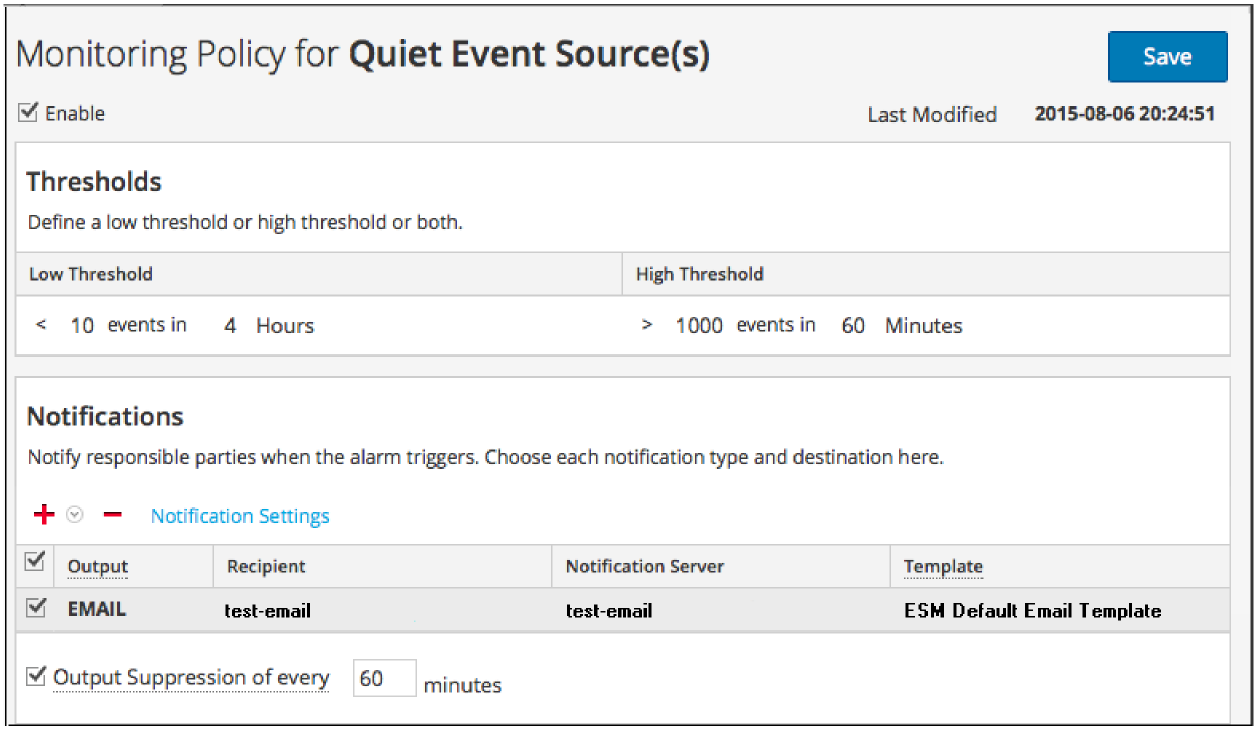
   > **Note:** Default ESM (Event Source Monitoring) templates are provided for each type of notification.

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)**

☑ 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.

☑	Output	Recipient	Notification Server	Template
☑	**EMAIL**	**test-email**	**test-email**	**ESM Default Email Template**

☑ Output Suppression of every 60 minutes

Disabling 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 Alarms Tab

Disable Notifications

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

1. Go to **(Admin) > 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.

Configuring Automatic Alerting

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

Prerequisites

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

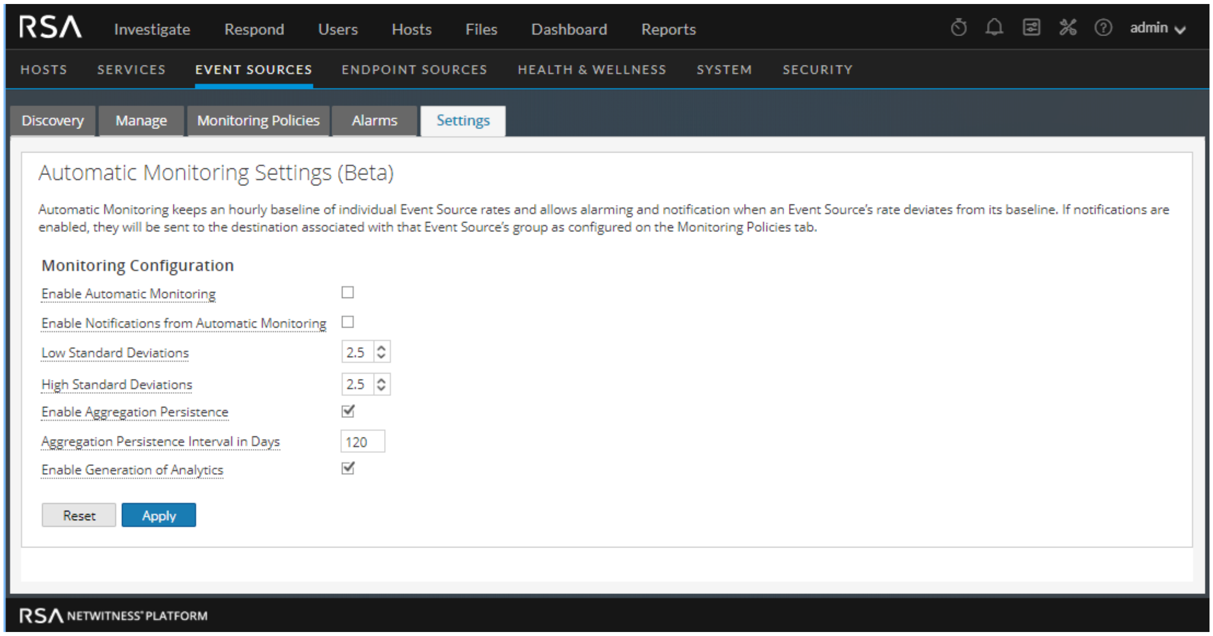
- **Notification Servers:** These are the servers that you want to receive notifications from the system. For more details, see the **Notification Servers Overview** topic in the *System Configuration Guide*.
- **Notification Templates:** These are the available templates for each type of notification. 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

To configure automatic alerting:

1. Go to **(Admin) > Event Sources**.
2. Select the **Settings** tab.

   The Settings tab is displayed.



Automatic Monitoring Settings (Beta)

Automatic Monitoring keeps an hourly baseline of individual Event Source rates and allows alarming and notification when an Event Source's rate deviates from its baseline. If notifications are enabled, they will be sent to the destination associated with that Event Source's group as configured on the Monitoring Policies tab.

Monitoring Configuration

Enable Automatic Monitoring □

Enable Notifications from Automatic Monitoring □

Low Standard Deviations 2.5

High Standard Deviations 2.5

Enable Aggregation Persistence ☑

Aggregation Persistence Interval in Days 120

Enable Generation of Analytics ☑

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 **2.5** (95% confidence).
   - **High Standard Deviations**: standard deviations above which to receive alerts. Default is **2.5** (95% confidence).

   Note: You can adjust the standard deviation settings in increments of 0.1 (one tenth) of a standard deviation.
6. Click **Save** to close the dialog and save your settings.

Viewing Event Source Alarms

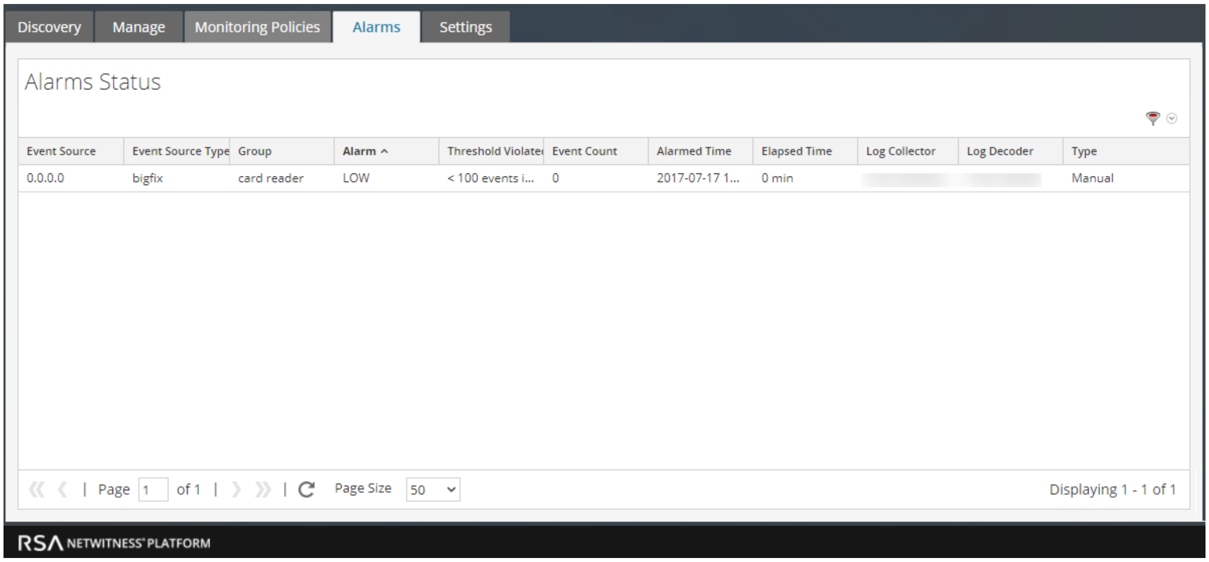
This topic describes how to view alarms for your event source groups. After you have configured and set alerts, you can view all of the generated alarms in the **Alarms** tab of the **Event Sources** view.

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. Go to **(Admin) > 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.



Alarms Status

Event Source	Event Source Type	Group	Alarm ^	Threshold Violatei	Event Count	Alarmed Time	Elapsed Time	Log Collector	Log Decoder	Type
0.0.0.0	bigfix	card reader	LOW	< 100 events i...	0	2017-07-17 1...	0 min	[redacted]	[redacted]	Manual

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.

Event Source Management References

The following topics contain reference information for Event Source Management:

- Discovery Tab
- Manage Tab
- Manage Event Source Tab
- Event Sources View
- Create/Edit Group Form
- Details View
- Historical Graph for System Stats
- Manage Parser Mappings
- Alarms Tab
- Monitoring Policies Tab
- Settings Tab

Discovery Tab

To access the Discovery tab, go to NetWitness (Admin) > **Event Sources**. The Discovery tab is displayed.

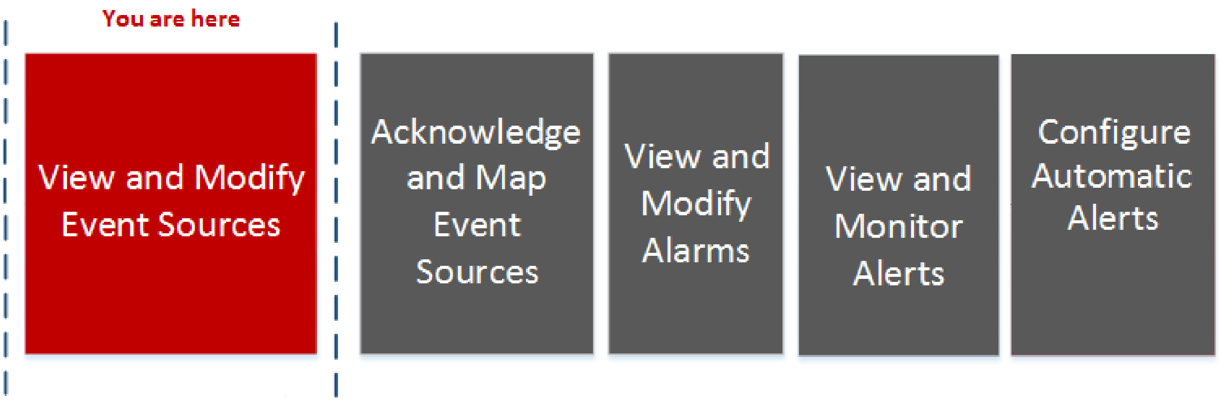
The Discovery tab lets you review the event source types that NetWitness has discovered for each address and the system's confidence of how likely it is that they were identified completely accurately. If the discovered event source types are correct, you can acknowledge to filter out that event source. If incorrect, you can set the allowed event source types for a particular address so that future logs will parse against the correct parsers.

Note: The following features apply to NetWitness version 11.1 and later:
- Acknowledging multiple event sources
- Filtering by event source type
- (for 11.2 and later) Mapping filter options include None, Auto, and Manual
- Mapping multiple event sources
- Searching for event sources on the Event Source Discovery page

NetWitness, version 11.2 and later, automatically maps incoming events to a type based on previous logs received from that address, reducing the mis-parsing of messages and reducing the number of items that need attention in the Discovery workflow. A value of **Auto** in the **Mapping Type** column indicates that an address has been auto-mapped.

Workflow

This workflow shows the overall process for configuring event sources.


You are here
View and Modify Event Sources
Acknowledge and Map Event Sources
View and Modify Alarms
View and Monitor Alerts
Configure Automatic Alerts

What do you want to do?

Role	I want to...	Documentation
Administrator	Acknowledge and map event sources.*	Acknowledging and Mapping Event Sources
Administrator	Add and configure parser mappings for a Log Decoder.*	Manage Parser Mappings
Administrator	View event source alarms.	Viewing Event Source Alarms
Administrator	Troubleshoot event source management.	ESM Troubleshooting & Appendix

*You can perform this task here.

Related Topics

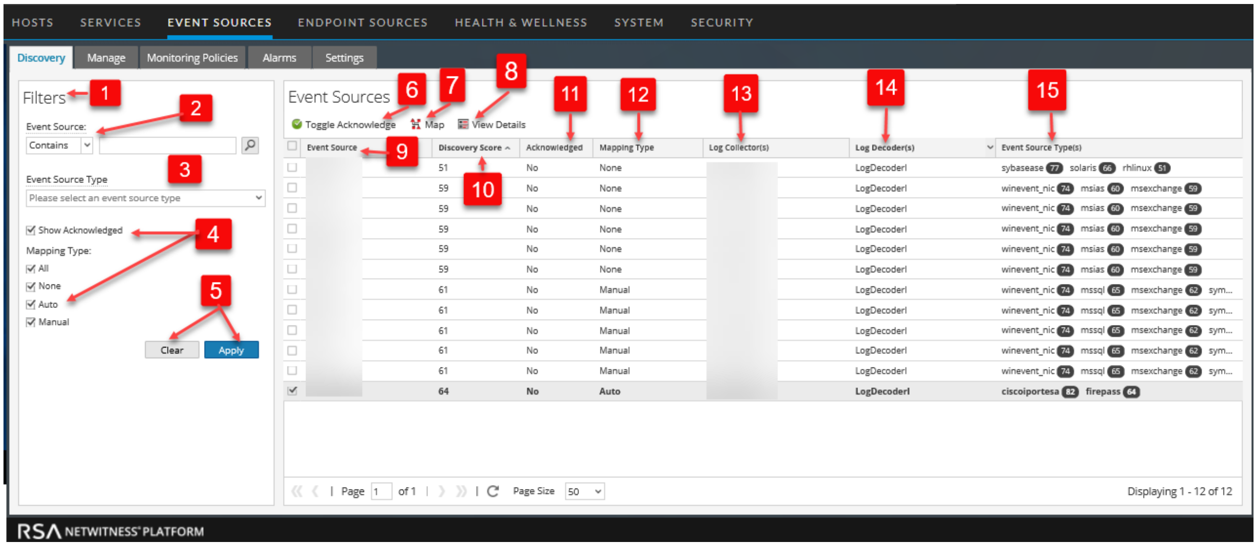
Manage Parser Mappings

Details View

Quick Look

The following example displays a list of addresses and their discovered Event Source types. The Event Source types display the Event Sources that have been discovered.

This is an example of the tab.



Event Source: Contains

Event Source Type: Please select an event source type

☑ Show Acknowledged

Mapping Type:

☑ All

☑ None

☑ Auto

☑ Manual

□	Event Source	Discovery Score	Acknowledged	Mapping Type	Log Collector(s)	Log Decoder(s)	Event Source Type(s)
□		51	No	None		LogDecoderI	sybasease 77 solaris 66 rhlinux 51
□		59	No	None		LogDecoderI	winevent_nic 74 msias 60 msexchange 59
□		59	No	None		LogDecoderI	winevent_nic 74 msias 60 msexchange 59
□		59	No	None		LogDecoderI	winevent_nic 74 msias 60 msexchange 59
□		59	No	None		LogDecoderI	winevent_nic 74 msias 60 msexchange 59
□		59	No	None		LogDecoderI	winevent_nic 74 msias 60 msexchange 59
□		61	No	Manual		LogDecoderI	winevent_nic 74 mssql 65 msexchange 62 sym...
□		61	No	Manual		LogDecoderI	winevent_nic 74 mssql 65 msexchange 62 sym...
□		61	No	Manual		LogDecoderI	winevent_nic 74 mssql 65 msexchange 62 sym...
□		61	No	Manual		LogDecoderI	winevent_nic 74 mssql 65 msexchange 62 sym...
□		61	No	Manual		LogDecoderI	winevent_nic 74 mssql 65 msexchange 62 sym...
☑		**64**	**No**	**Auto**		**LogDecoderI**	**ciscoiportesa 82 firepass 64**

Page 1 of 1 Page Size 50 Displaying 1 - 12 of 12

1 Displays the Filters and Event Sources panels with the Discovery tab open.

2 Displays the Event Source Filter field with a drop-down menu that offers the following options:

- Enter the full or partial address (IP, IPv6 or Hostname) of the source(s) you want to review. You can also enter multiple entries that are separated by commas.
  For example, **10.10.10.10,10.10.10.11,host1.company.com**
- **Exact:** Returns sources that completely match the search term.
  For example, **10.10.10.10** only returns **10.10.10.10**, not **10.10.10.101**.
- **Starts With:** Returns sources that start with the search term.
  For example,**10.10.10.** returns the whole **10.10.10.x subnet**.
- **Contains:** Returns sources that start with the search term.
  For example, **exch** returns all terms such as **us-exch-1.company.com**, or **lab21** returns all **hostx.lab21.company.com** terms.
- **Ends With:** Returns sources that end with the search term.
  For example, **lab21.company.com** returns all hosts.

Note: When specifying the search string, you can use **. - :** (period, dash, colon).

3 The Event Source Type drop-down menu filters for addresses containing all of the selected event source types.

4
- Select the **Show Acknowledged** checkbox to display acknowledged Event Sources.
- Mapping filter options can include just one of the mapping types listed in the Filter Panel, or multiple Mapping Types can be selected.

Note: If no mapping filter options are selected, the default is to display **All**, **None**, **Manual**, and **Auto** mapping types.

5
- The **Apply** button uses all criteria that is set in all filters.
- The **Clear** button clears all filters from the panel.

6 Toggles the event sources between acknowledged and not acknowledged states.

7 Maps the selected event sources.

8 View Details button to view details of the selected Event Source.

9 Displays the addresses of the selected Event Sources.

10 Displays the discovery scores of the selected Event Sources.

11 Displays whether or not the selected Event Sources have been acknowledged.

12 Displays the selected Event Source Mapping type as Auto, Manual, or None. Any changes to the mapping are only displayed here.

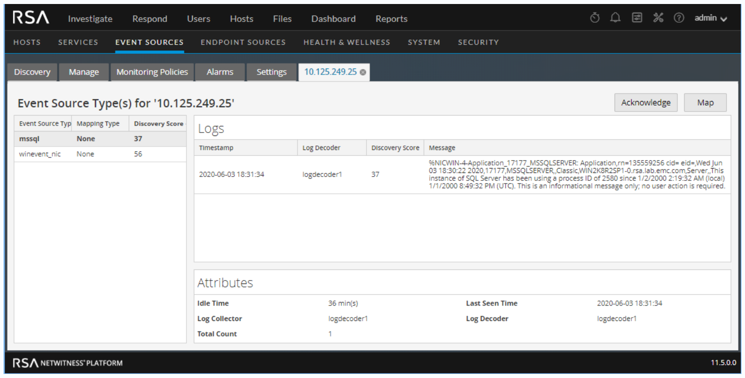
13 Displays the host names of the Log Collectors where the Event Sources are located.

14 Displays the host names of the Log Decoders where the Event sources are located.

15 Displays the discovered Event Source Types and their associated discovery scores.

Toolbar and Features

The Discovery tab contains the following features:

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td><b>Tools</b>
✓ Toggle Acknowledge
Map</td><td>The following items are available on the toolbar:
<ul>
<li><b>Toggle Acknowledge</b>: Toggles the acknowledged state for the selected Event Source between <b>Yes</b> and <b>No</b>.</li>
<li><b>Map</b>: Opens the Manage Parser Mappings dialog box, where you can map an event source to the correct log parser.</li>
<li><b>View Details</b>: Provides details on the selected Event Source, as well as logs that have been received for this event source. For example:</li>
</ul>

RSA
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
admin
HOSTS
SERVICES
EVENT SOURCES
ENDPOINT SOURCES
HEALTH &amp; WELLNESS
SYSTEM
SECURITY
Discovery
Manage
Monitoring Policies
Alarms
Settings
10.125.249.25
Acknowledge
Map
RSA NETWITNESS® PLATFORM
11.5.0.0
Event Source Type(s) for '10.125.249.25'
<table>
<tr><th>Event Source Typ</th><th>Mapping Type</th><th>Discovery Score</th></tr>
<tr><td>mssql</td><td>None</td><td>37</td></tr>
<tr><td>winevent_nic</td><td>None</td><td>56</td></tr>
</table>
Logs
<table>
<tr><th>Timestamp</th><th>Log Decoder</th><th>Discovery Score</th><th>Message</th></tr>
<tr><td>2020-06-03 18:31:34</td><td>logdecoder1</td><td>37</td><td>%NICWIN-4-Application_17177_MSSQLSERVER: Application,rn=135559256 cid= eid=,Wed Jun 03 18:30:22 2020,17177,MSSQLSERVER,,Classic,WIN2K8R2SP1-0.rsa.lab.emc.com,Server,,This instance of SQL Server has been using a process ID of 2580 since 1/2/2000 2:19:32 AM (local) 1/1/2000 8:49:32 PM (UTC). This is an informational message only; no user action is required.</td></tr>
</table>
Attributes
<table>
<tr><td>Idle Time</td><td>36 min(s)</td><td>Last Seen Time</td><td>2020-06-03 18:31:34</td></tr>
<tr><td>Log Collector</td><td>logdecoder1</td><td>Log Decoder</td><td>logdecoder1</td></tr>
<tr><td>Total Count</td><td>1</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td><b>Event Source</b></td><td>The IP, IPv6, or Hostname of the Event Source.</td></tr>
<tr><td><b>Discovery Score</b></td><td>Displays the overall discovery score associated with that particular address. Higher scores indicate better confidence. Discovery scores range from 0 (least confident) to 100 (most confident).</td></tr>
<tr><td><b>Acknowledged</b></td><td>Selections are either <b>Yes</b> (you have acknowledged the Event Source) or
<b>No</b> (you have not acknowledged the Event Source).</td></tr>
</table>

Field	Description
Mapping Type	Selections are **Manual** (you mapped the Event Source), **Auto** (the system automatically mapped the Event Source), or **None** (you have not mapped the Event Source). Auto mapping is content aware. When a log message is parsed to a high confidence header or message that has been tagged, an auto mapping will be set for that address and type. This auto-mapping is valid for 24 hours and will be renewed every time a log message matches a tagged header of a message. Log messages are first parsed against auto-mapped parsers, and only fall back to discovery if there is no match amongst the mapped parsers. Log messages that fall back to discovery can match the tagged headers or messages from other event sources: this results in multiple types being mapped. For example, an address could eventually be mapped to Windows, MS SQL, and Apache, and these parsers are evaluated first. If an event source is decommissioned, and its IP re-purposed, the 24-hour timer ages out the mappings for the decommissioned types. **Note:** This features applies to RSA NetWitness version 11.2 and later.
Log Collector(s)	Log Collectors that have received logs from this Event Source address.
Log Decoder(s)	Log Decoders that have received logs from this Event Source address.
Event Source Type(s)	The parsed type(s) of the Event Source address and the corresponding Discovery Score for each type.

Note: Discovery Scores are only available for 11.0 and above Log Decoders. Discovery Scores for pre-11.0 Log Decoders display as Unavailable.

The following table describes the sorting order for discovery scores. To access the Sorting Order drop-down menu, click on the down arrow in the Event Sources column.

Field	Description
Sort Ascending	Sort the column by discovery score in ascending order.
Sort Descending	Sort the column by discovery score in descending order.
Columns	Used to hide or show one or more columns.

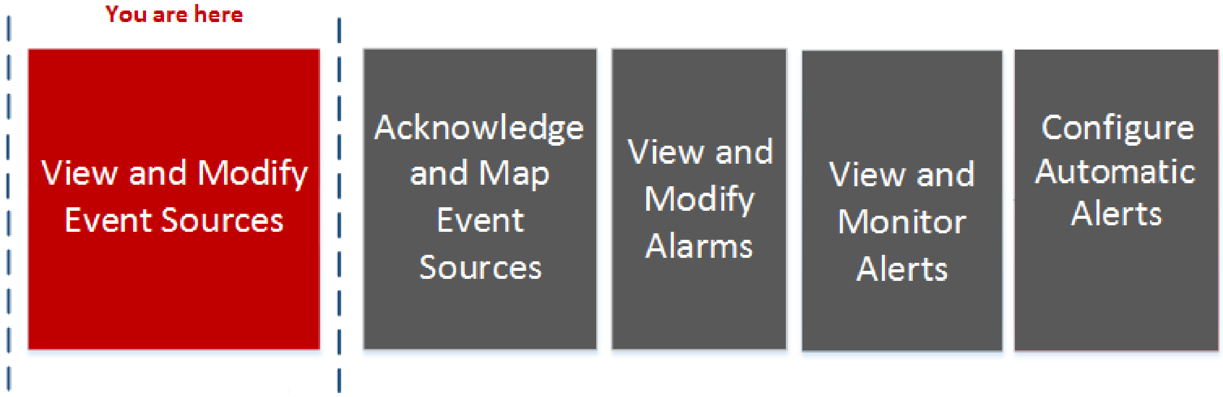
Manage Tab

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

To access this tab, go to ✂ (Admin) > **Event Sources** > **Manage**.

Workflow

This workflow shows the overall process for configuring event sources.


You are here
View and Modify Event Sources
Acknowledge and Map Event Sources
View and Modify Alarms
View and Monitor Alerts
Configure Automatic Alerts

What do you want to do?

Role	I want to...	Documentation
Administrator	*View and modify event sources.	Managing Event Source Groups
Administrator	Acknowledge and map event sources.	Acknowledging and Mapping Event Sources
Administrator	Add and configure parser mappings for a Log Decoder	Manage Parser Mappings
Administrator	View event source alarms.	Viewing Event Source Alarms
Administrator	Troubleshoot event source management.	ESM Troubleshooting & Appendix

*You can perform this task here.

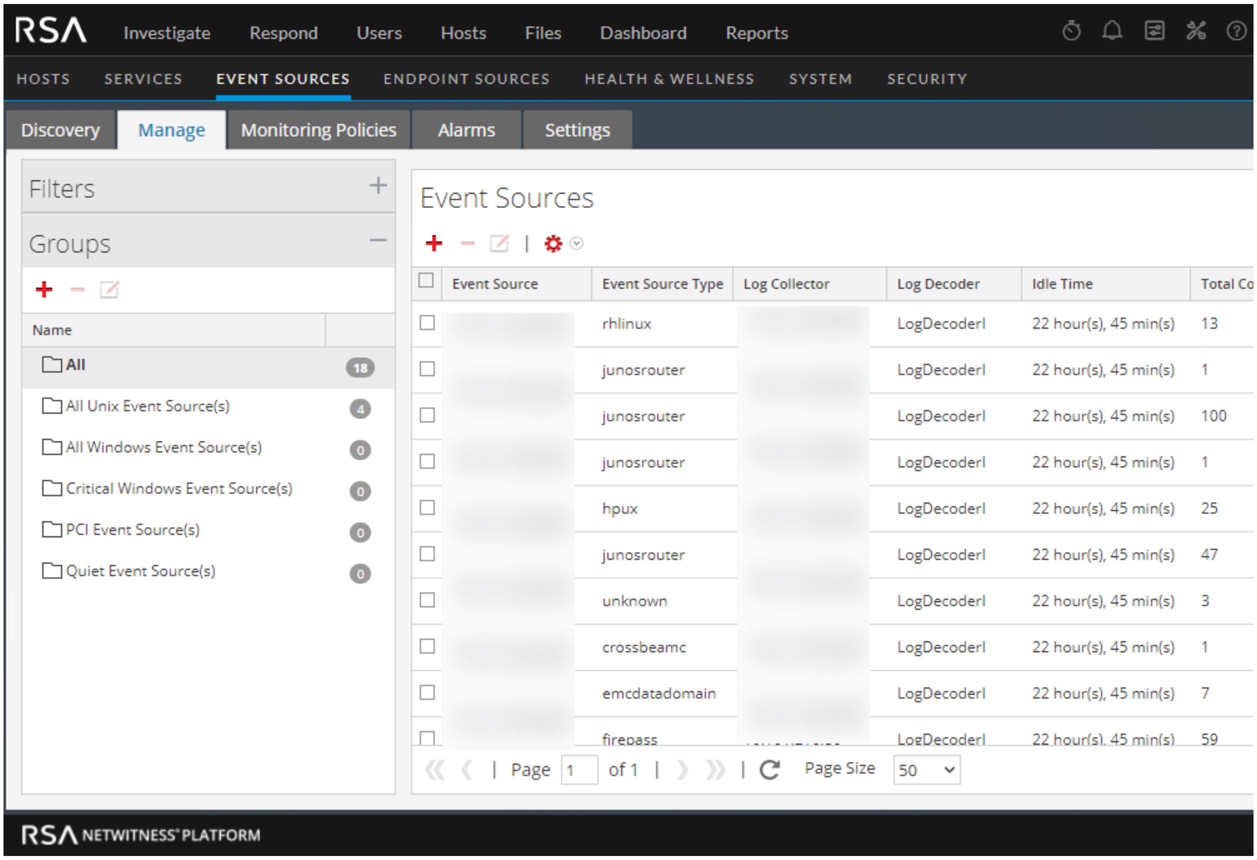
Related Topics

Creating Event Source Groups

Creating an Event Source and Editing Attributes

Quick Look

The Manage tab organizes event sources into groups, and displays attributes for each event source. The Manage tab consists of two panels, Groups and Event Sources.

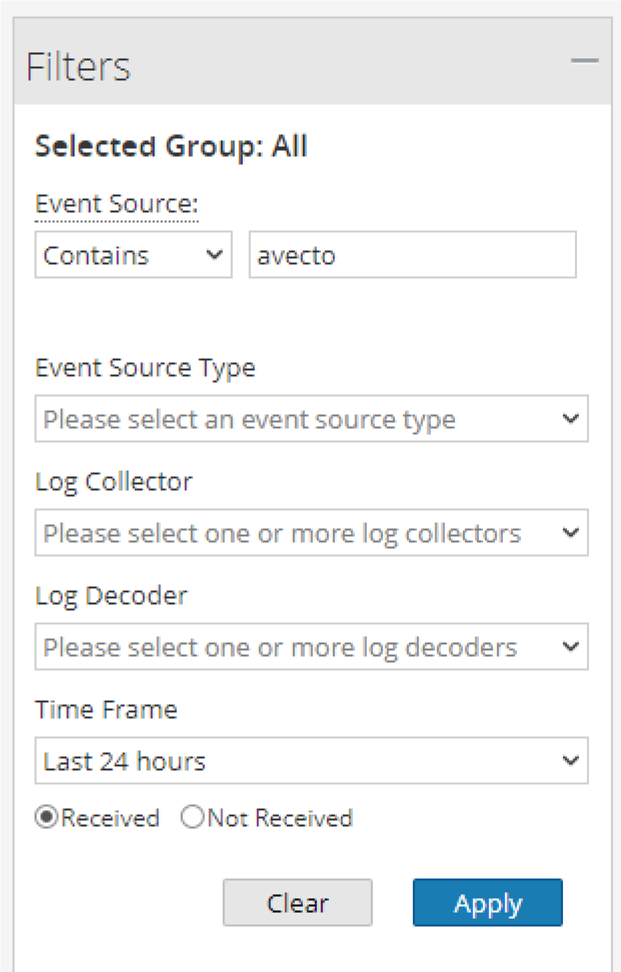


Name	
All	18
All Unix Event Source(s)	4
All Windows Event Source(s)	0
Critical Windows Event Source(s)	0
PCI Event Source(s)	0
Quiet Event Source(s)	0

□	Event Source	Event Source Type	Log Collector	Log Decoder	Idle Time	Total Co
□	[redacted]	rhlinux	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	13
□	[redacted]	junosrouter	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	1
□	[redacted]	junosrouter	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	100
□	[redacted]	junosrouter	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	1
□	[redacted]	hpux	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	25
□	[redacted]	junosrouter	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	47
□	[redacted]	unknown	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	3
□	[redacted]	crossbeamc	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	1
□	[redacted]	emcdatadomain	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	7
□	[redacted]	firepass	[redacted]	LogDecoderl	22 hour(s), 45 min(s)	59

Filter Panel

The Filter Panel provides options for filtering the set of event sources shown in the grid view. This is an example of the Filter Panel:



Filters

Selected Group: All

Event Source:

Contains | avecto

Event Source Type

Please select an event source type

Log Collector

Please select one or more log collectors

Log Decoder

Please select one or more log decoders

Time Frame

Last 24 hours

● Received ○ Not Received

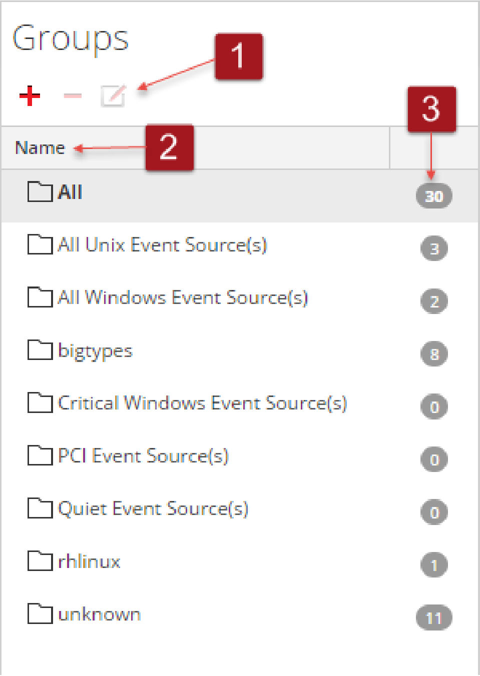
This panel provides the following options:

- You can filter on the event source name, using **Contains**, **Exact**, **Starts With**, or **Ends With**. Select one of these choices, then enter the corresponding string to match against.
- Select one or more Event Source Types to filter based on this value.
- To view event sources that send data to a particular Log Collector, select a Log Collector from the drop-down list.
- To view event sources that send data a particular Log Decoder, select a Log Decoder from the drop-down list.
- Select the time frame for when the events were collected. You can choose a value from 5 minutes to the previous 90 days, or all data that has been collected.
- Use the **Received** and **Not Received** radio buttons to filter the query results to contain only event sources that logs have been received from within the selected time, or query results to contain only event sources that logs have not been received from within the selected time.

After you complete the set of filters, click **Apply** to view the query results in the Event Sources grid.

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.

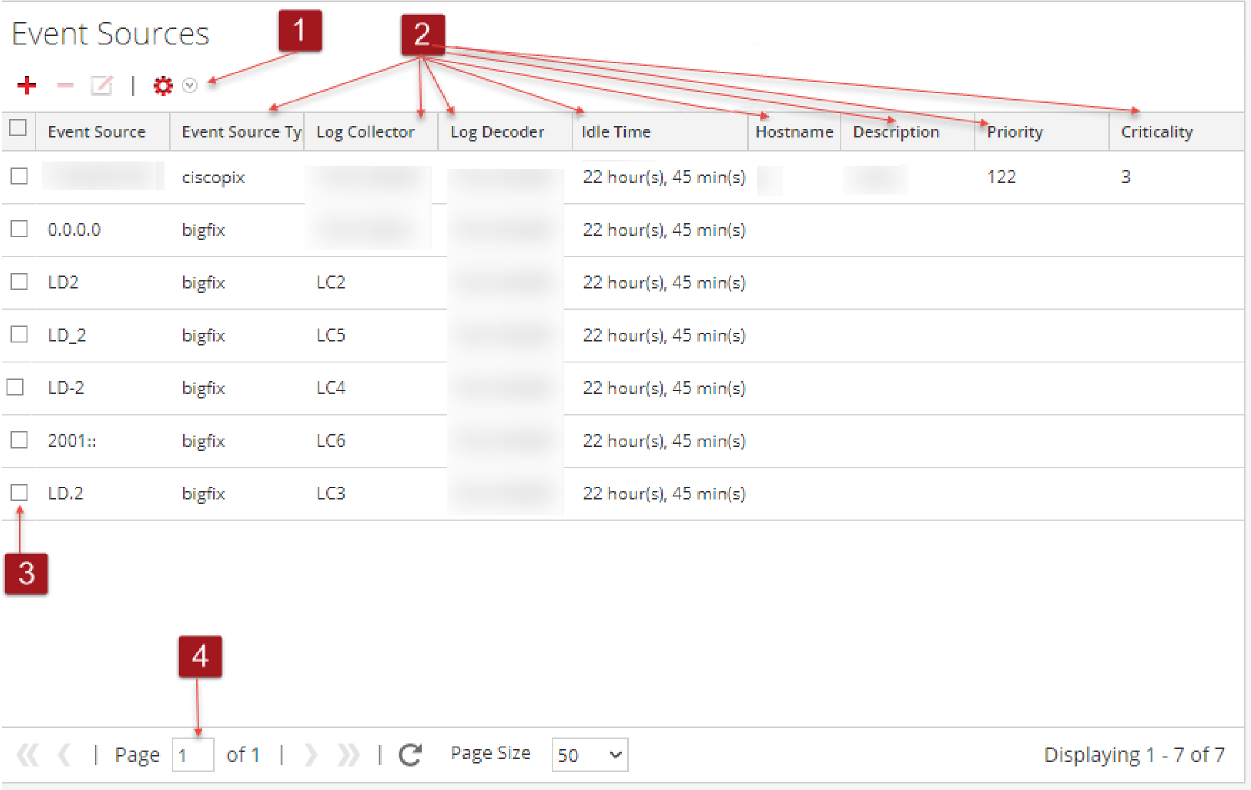


Name	
All	30
All Unix Event Source(s)	3
All Windows Event Source(s)	2
bigtypes	8
Critical Windows Event Source(s)	0
PCI Event Source(s)	0
Quiet Event Source(s)	0
rhlinux	1
unknown	11

1	Displays the standard NetWitness icons for adding, removing, or editing groups.
2	Lists the identifier for each group in the Name column. You can use the group names to quickly identify some of the criteria used to form the group. 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**. **Note:** The event source group name is not editable. After you create a group, that name exists as long as the group itself.
3	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. **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.

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 Source	Event Source Ty	Log Collector	Log Decoder	Idle Time	Hostname	Description	Priority	Criticality
□	[redacted]	ciscopix	[redacted]	[redacted]	22 hour(s), 45 min(s)	[redacted]	[redacted]	122	3
□	0.0.0.0	bigfix	[redacted]	[redacted]	22 hour(s), 45 min(s)				
□	LD2	bigfix	LC2	[redacted]	22 hour(s), 45 min(s)				
□	LD_2	bigfix	LC5	[redacted]	22 hour(s), 45 min(s)				
□	LD-2	bigfix	LC4	[redacted]	22 hour(s), 45 min(s)				
□	2001::	bigfix	LC6	[redacted]	22 hour(s), 45 min(s)				
□	LD.2	bigfix	LC3	[redacted]	22 hour(s), 45 min(s)				

1 The toolbar contains the following tools:

- **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:
  - **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.

2 Columnar display of attributes. You can choose which attributes to display.

3 Checkboxes: Select rows to use when performing tasks on multiple event sources, such as bulk editing.

4 Navigation Tools:

At the bottom of the screen, there are items that help in navigating your group:

- **Page *x* of *y***: 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 *x* - *y* of *z***: 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

Historical Graph for System Stats

Note: The information in this topic applies to NetWitness Version 11.4.1 and later.

Historical system statistics are available for each event source.

To access the Historical Graph for the System Stats:

1. Go to 🛠 **(Admin) > Event Sources**.

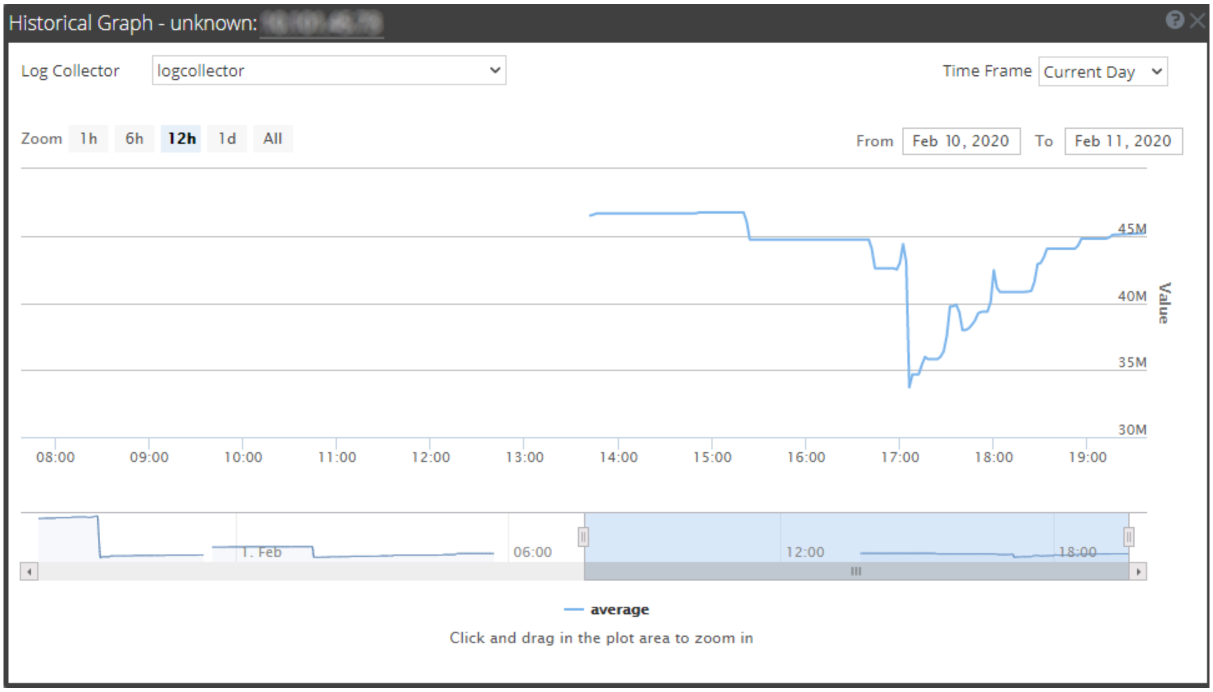
   The Event Sources view is displayed.

2. Click the **Manage** tab.

   The Event Sources Manage tab is displayed.

3. In the **Historical Graph** column, select the view chart icon (📊) for any listed event source.

   The Historical graph for the selected event source is displayed. The figure displays event source activity.



Historical Graph - unknown: [redacted]

Log Collector logcollector

Time Frame Current Day

Zoom 1h 6h 12h 1d All

From Feb 10, 2020 To Feb 11, 2020

Parameters

You can customize the graph view as required. The table lists the various parameters used to customize the historical graph view.

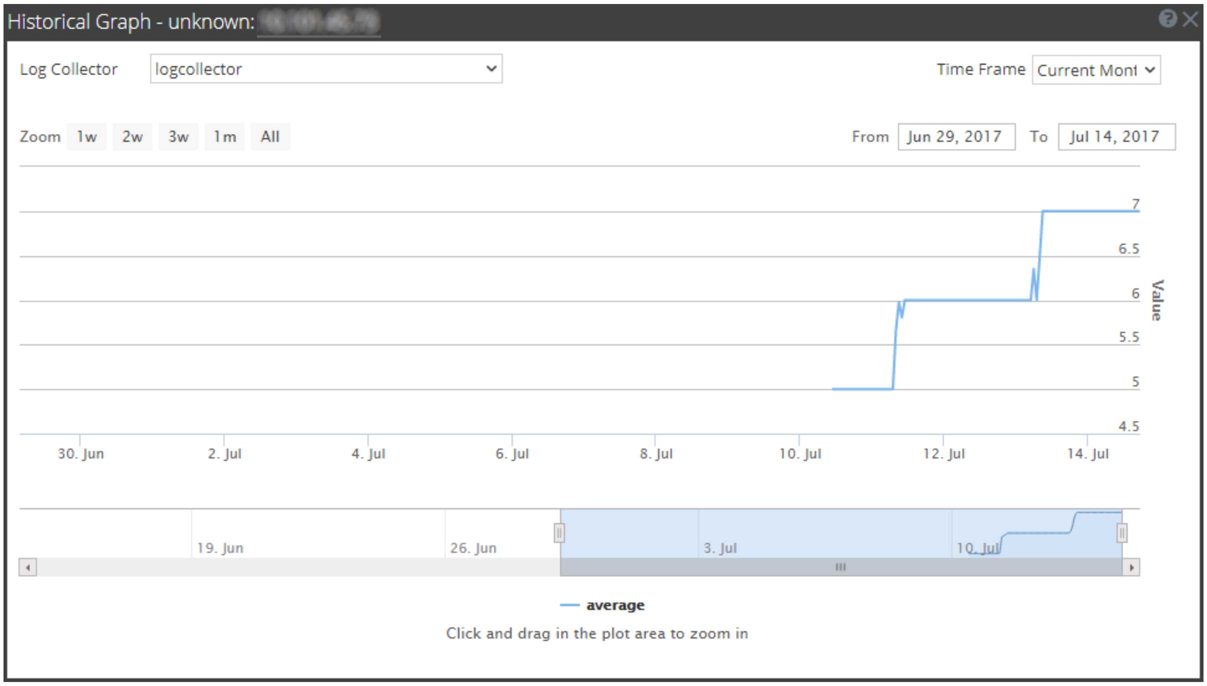
Parameter	Description
Log Collector	Select the Log Collector for which you want to view historical data. In some cases, the historical data for an event source may be spread across multiple Log Collectors.
Time Frame	Select the time frame for which you want to view the historical data. The available options are: **Current Day**, **Current Week**, **Current Month**, and **Current Year**.
From <date> To <date>	Select the date range for which you want to view the historical data.

You can zoom in for a detailed view of the data in the Historical graph.

Examples of Zooming In

You can select one of the values to view the historical data for the selected value. The figure below displays an example for the 6 hour frame selected for zoom in. The slider bar at the right bottom corner is also changed to a 6 hour window.

Alternatively, you can slide the bar in the right hand corner to zoom in to a required frame.



Historical Graph - unknown: [redacted]

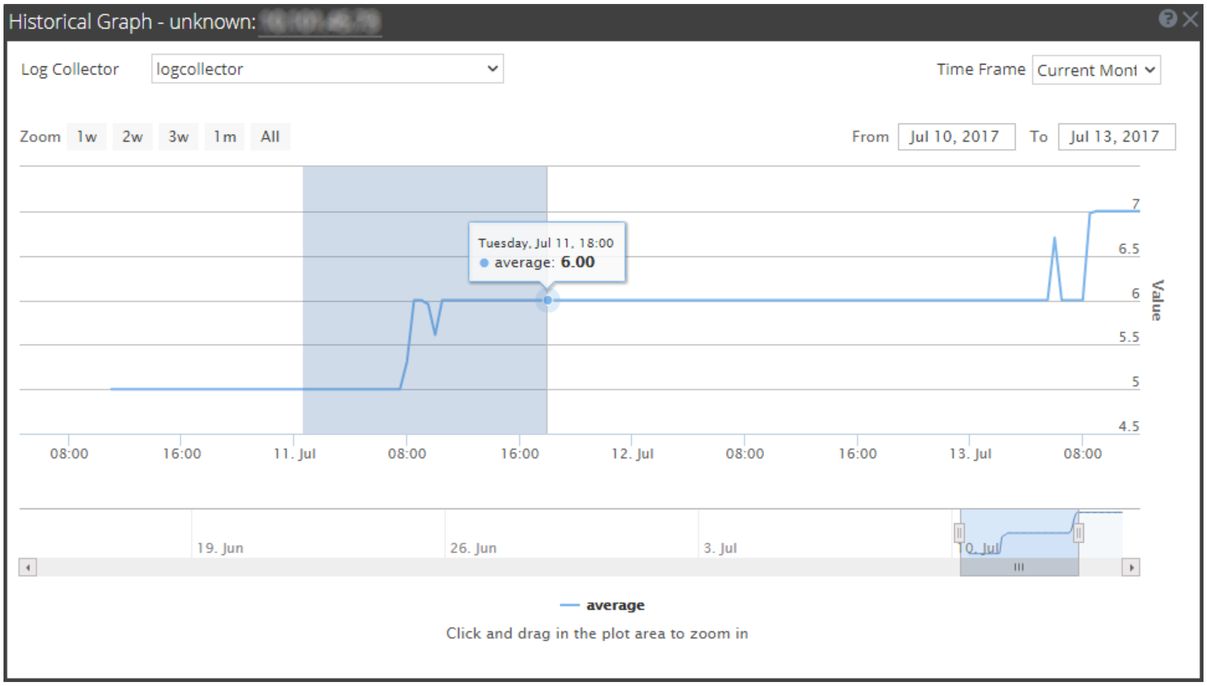
Log Collector: logcollector

Time Frame: Current Mont

From: Jun 29, 2017 To: Jul 14, 2017

You can click and drag in the plot area to zoom in for a required frame of time.

The figure below displays an example of how the graph appears while you click and drag.



Historical Graph - unknown: [redacted]

Log Collector: logcollector

Time Frame: Current Mont

From: Jul 10, 2017 To: Jul 13, 2017

Tuesday, Jul 11, 18:00
● average: **6.00**

Manage Event Source Tab

The Manage Event Source screen has several integrated components that present different perspectives of an event source.

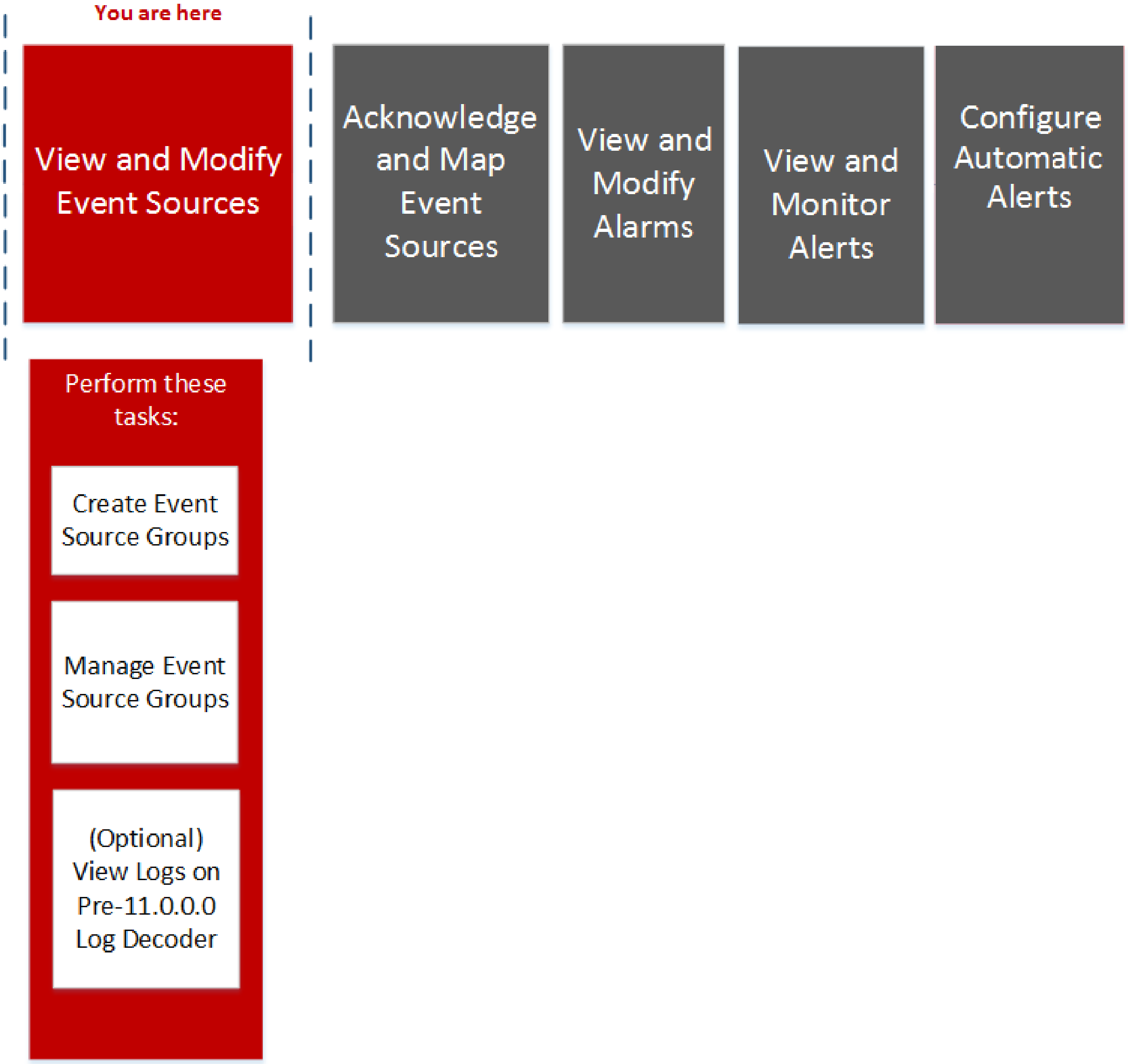
- Show Event Source Details
- Add attribute values to an event source
- Remove attribute values for an event source

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

1. Go to **(Admin) > Event Sources**.
2. Select the **Manage** tab.
3. From the Event Sources pane, select an event source from the list and click + .

Workflow

This workflow shows the end-to-process for modifying, acknowledging, mapping, and configuring event sources, along with viewing and configuring event source alarms and alerts.


You are here
View and Modify Event Sources
Acknowledge and Map Event Sources
View and Modify Alarms
View and Monitor Alerts
Configure Automatic Alerts
Perform these tasks:
Create Event Source Groups
Manage Event Source Groups
(Optional) View Logs on Pre-11.0.0.0 Log Decoder

What do you want to do?

Role	I want to...	Documentation
Administrator	Create an event source group that contains all the high priority event sources.	Creating Event Source Groups
Administrator	Edit event source attributes.	Creating an Event Source and Editing Attributes

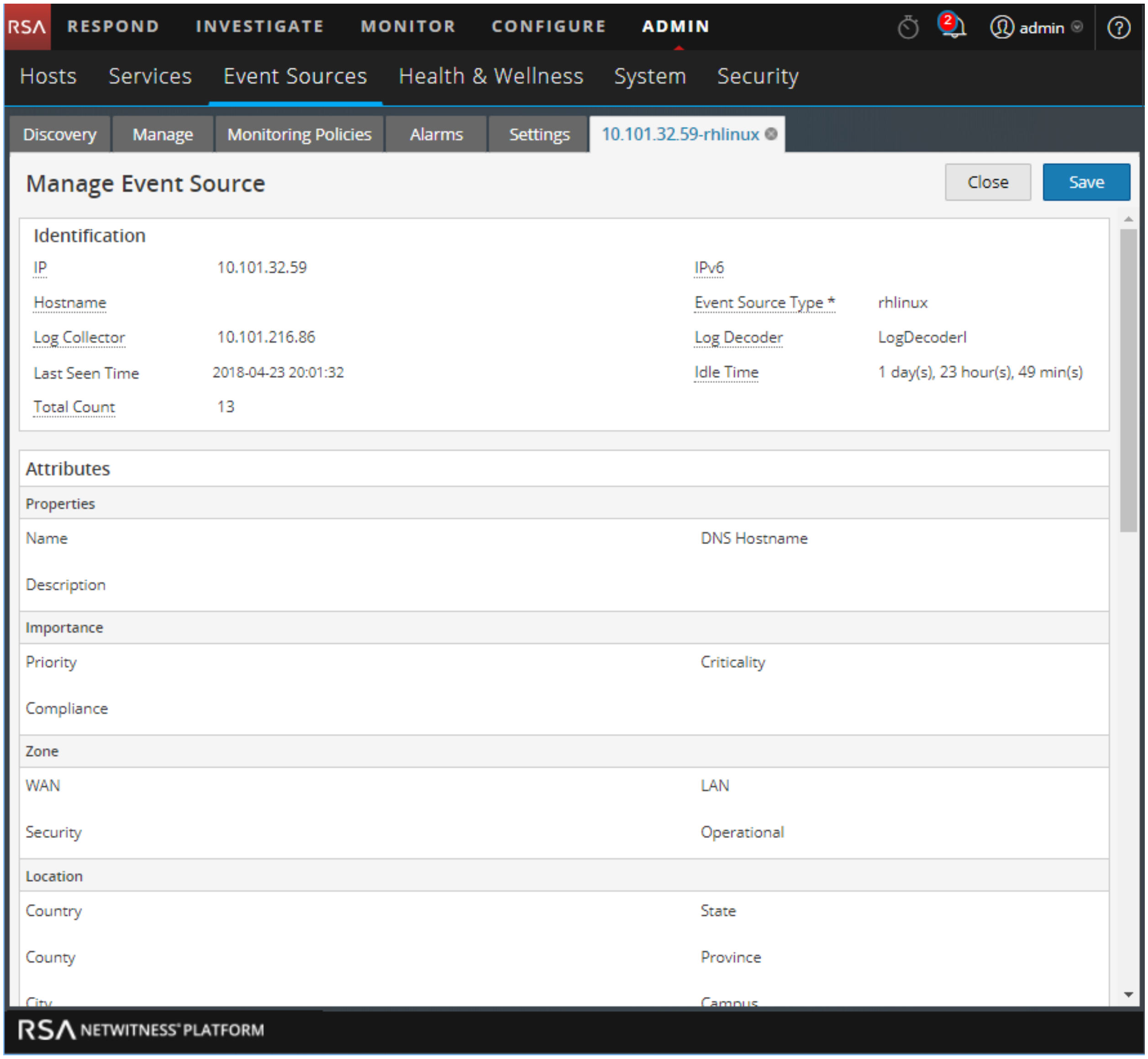
Related Topics

Creating Event Source Groups

Creating an Event Source and Editing Attributes

Quick Look

This is an example of the Event Source tab:



Manage Event Source

Identification

IP	10.101.32.59	IPv6	
Hostname		Event Source Type *	rhlinux
Log Collector	10.101.216.86	Log Decoder	LogDecoderl
Last Seen Time	2018-04-23 20:01:32	Idle Time	1 day(s), 23 hour(s), 49 min(s)
Total Count	13		

Attributes

Properties

Name	DNS Hostname
Description	

Importance

Priority	Criticality
Compliance	

Zone

WAN	LAN
Security	Operational

Location

Country	State
County	Province
City	Campus

This table describes event source attribute categories.

Attribute Section	Description
Identification	These attributes are the main attributes that collectively identify an event source. You can only change these attributes when you are specifying the details for a new event source. For an existing event source, the attributes in this section are auto-populated, and cannot be changed while on this screen. Attributes available for a new event source: • IP • IPv6 • Hostname • Event Source Type • Log Collector • Log Decoder The following attributes are displayed when viewing the details for an existing event source: • Last Seen Time: this is the last time there was communication between NetWitness and the event source • Idle Time: this is the amount of time elapsed since the **Last Seen Time**. This time can be useful if you want to filter event sources that have been inactive for a certain duration. • Total Count: total count of all event sources for this **Event Source Type**.
Properties	These attributes provide the name and description. • Name • DNS Hostname • Description
Importance	These attributes can be used for grouping by priority. • Priority • Criticality • Compliance

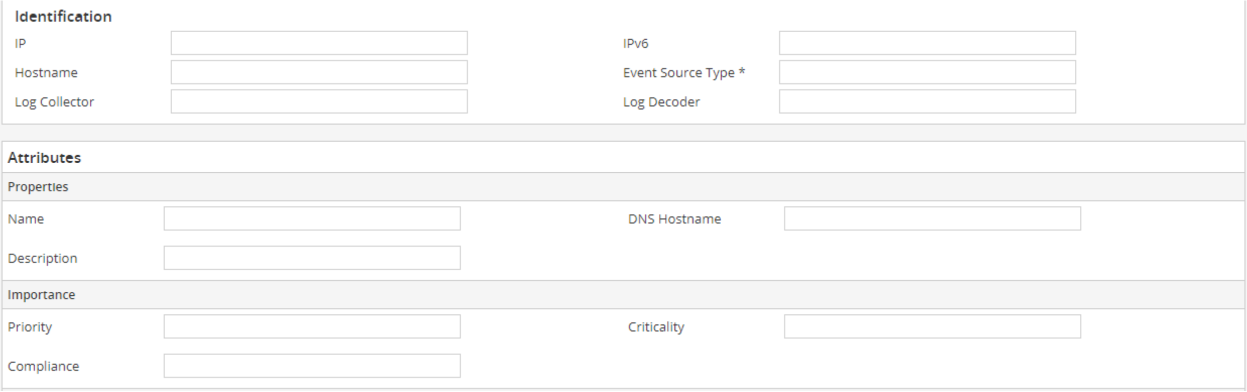
Attribute Section	Description
Zone	These attributes can be used for grouping by zone. • WAN (Wide Area Network) • LAN (Local Area Network) • Security • Operational
Location	These attributes can be used to group by the physical or geographical location. • Country • State • County • Province • City • Campus • Postal Code • Building • Floor • Room
Organization	These attributes can be used to group by organization, and also to provide contact information. • Company • Division • Business Unit • Department • Group • Contact • Contact Phone • Contact Email
Owner	These attributes specify those responsible for the event source. • Manager • Primary Administrator • Backup Administrator

Attribute Section	Description
Physical	These attributes specify the physical properties for the event source. • Vendor • Serial Number • Asset Tag • Voltage • UPS Protected • Rack Height • Depth • BTU Output • Color
Function	These attributes can be used to group by function. • Primary Role • Sub Role 1 • Sub Role 2
System Information	These attributes specify system information. • Domain Name • System Name • Identifier • System Description
Custom	This section provides eight custom attributes, for any other attributes that your organization might need.

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 NetWitness, 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.



Identification

IP		IPv6	
Hostname		Event Source Type *	
Log Collector		Log Decoder	

Attributes

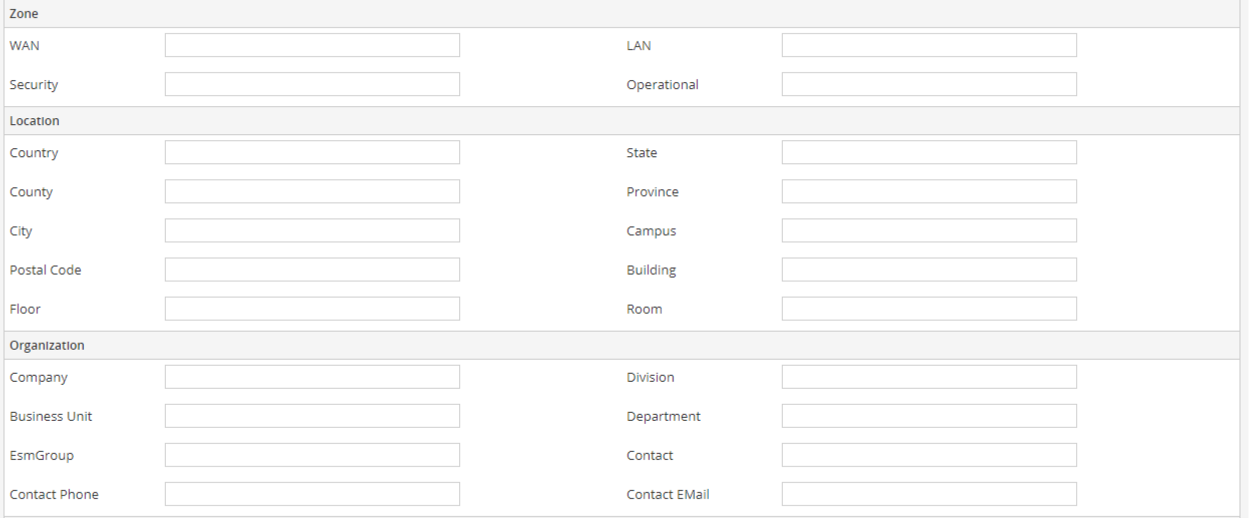
Properties

Name		DNS Hostname	
Description			

Importance

Priority		Criticality	
Compliance			

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



Zone

WAN		LAN	
Security		Operational	

Location

Country		State	
County		Province	
City		Campus	
Postal Code		Building	
Floor		Room	

Organization

Company		Division	
Business Unit		Department	
EsmGroup		Contact	
Contact Phone		Contact EMail	

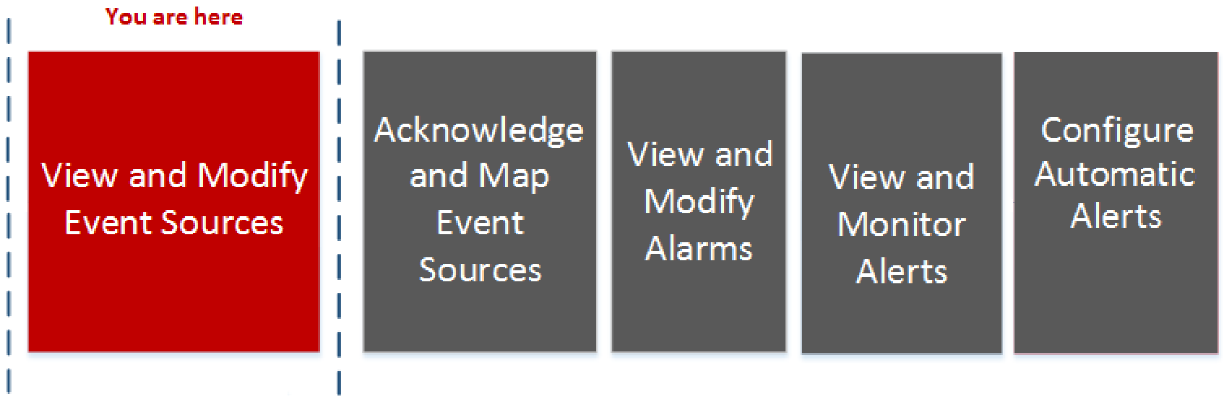
Event Sources View

The Event Source Attributes panel has the following tabs.

To access this panel, go to **(Admin) > Event Sources**.

Workflow

This workflow shows the end-to-process for modifying, acknowledging, mapping, and configuring event sources, along with viewing and configuring event source alarms and alerts.


You are here
View and Modify Event Sources
Acknowledge and Map Event Sources
View and Modify Alarms
View and Monitor Alerts
Configure Automatic Alerts

What do you want to do?

Role	I want to...	Documentation
Administrator	Create an event source group.	Creating Event Source Groups
Administrator	Edit or delete an event source group.	Editing or Deleting Event Source Groups
Administrator	Edit event source attributes.	Creating an Event Source and Editing Attributes

Related Topics

Managing Event Source Groups

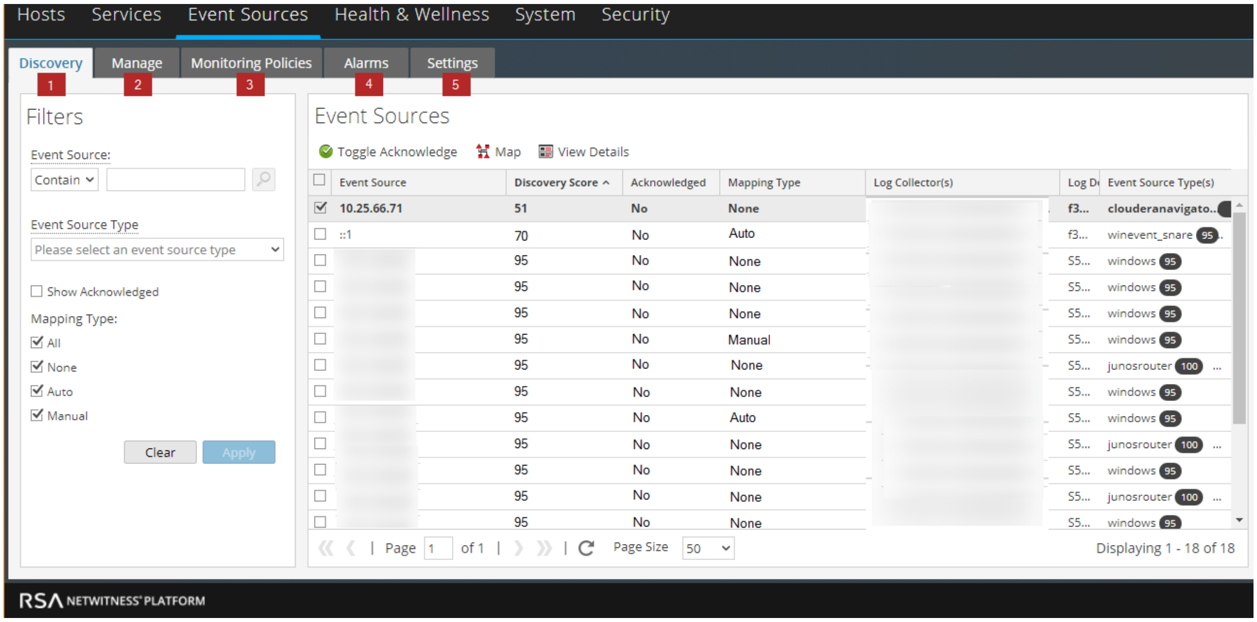
Creating Event Source Groups

Editing or Deleting Event Source Groups

Creating an Event Source and Editing Attributes

Quick Look

The Event Sources view presents the details for Event Sources that are discovered, acknowledged, or mapped by NetWitness.



Filters

Event Source: Contain

Event Source Type: Please select an event source type

□ Show Acknowledged

Mapping Type:
☑ All
☑ None
☑ Auto
☑ Manual

Clear | Apply

Event Sources

Toggle Acknowledge | Map | View Details

□	Event Source	Discovery Score ^	Acknowledged	Mapping Type	Log Collector(s)	Log De	Event Source Type(s)
☑	10.25.66.71	51	No	None	[redacted]	f3...	clouderanavigato...
□	::1	70	No	Auto	[redacted]	f3...	winevent_snare 95
□	[redacted]	95	No	None	[redacted]	S5...	windows 95
□	[redacted]	95	No	None	[redacted]	S5...	windows 95
□	[redacted]	95	No	None	[redacted]	S5...	windows 95
□	[redacted]	95	No	Manual	[redacted]	S5...	windows 95
□	[redacted]	95	No	None	[redacted]	S5...	junosrouter 100 ...
□	[redacted]	95	No	None	[redacted]	S5...	windows 95
□	[redacted]	95	No	Auto	[redacted]	S5...	windows 95
□	[redacted]	95	No	None	[redacted]	S5...	junosrouter 100 ...
□	[redacted]	95	No	None	[redacted]	S5...	windows 95
□	[redacted]	95	No	None	[redacted]	S5...	junosrouter 100 ...
□	[redacted]	95	No	None	[redacted]	S5...	windows 95

Page 1 of 1 | Page Size 50 | Displaying 1 - 18 of 18

1 Discovery Tab

Use this tab to review the event source types that NetWitness has discovered for each address and the system's confidence of how likely it is that they were identified accurately.

2 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.

3 Monitoring Policies Tab

Use this tab to manage alert configuration for event sources.

4 Alarms Tab

Use this tab to see the details of the alarms that have been generated.

5 Settings Tab

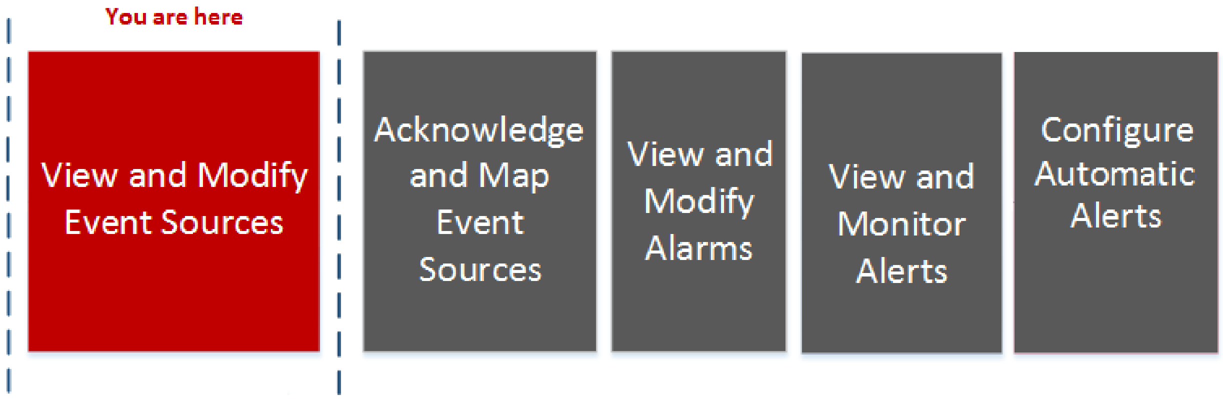
Use this tab to view or change the behavior for automatic (baseline) alerts.

Create/Edit Group Form

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

Workflow

This workflow shows the overall process for configuring event sources.


You are here
View and Modify Event Sources
Acknowledge and Map Event Sources
View and Modify Alarms
View and Monitor Alerts
Configure Automatic Alerts

What do you want to do?

Role	I want to...	Documentation
Administrator	*View and modify event sources.	Managing Event Source Groups
Administrator	Acknowledge and map events sources.	Acknowledging and Mapping Event Sources
Administrator	Add and configure parser mappings for a Log Decoder	Manage Parser Mappings
Administrator	View event source alarms.	Viewing Event Source Alarms
Administrator	Troubleshoot event source management.	ESM Troubleshooting & Appendix

*You can perform this task here.

Related Topics

Creating Event Source Groups

Managing Event Source Groups

Details View

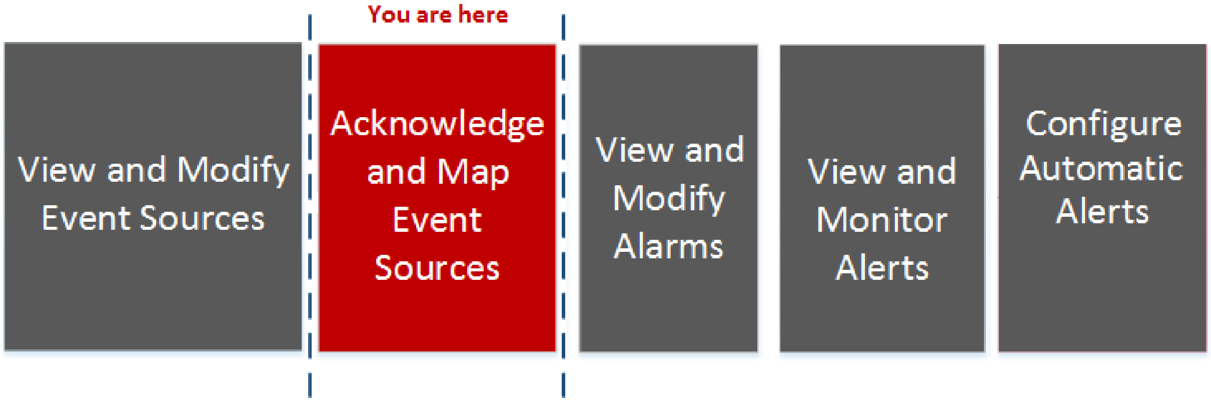
The **Details** view allows you to see details about the Event Source, as well as viewing a sample of the logs identified for each type in order to verify their accuracy.

You can access the **Details** view in a couple of ways.

- From the Toolbar, click the **View Details** button. Or, you can
- Double-click on the Event Source you selected.

Workflow

This workflow shows the overall process for configuring event sources.


You are here
View and Modify Event Sources
Acknowledge and Map Event Sources
View and Modify Alarms
View and Monitor Alerts
Configure Automatic Alerts

What do you want to do?

Role	I want to...	Documentation
Administrator	View and modify event sources.	Managing Event Source Groups
Administrator	*Acknowledge and map events sources.	Acknowledging and Mapping Event Sources
Administrator	Add and configure parser mappings for a Log Decoder	Manage Parser Mappings
Administrator	View log parser details	Manage Parser Mappings
Administrator	Troubleshoot event source management.	ESM Troubleshooting & Appendix

*You can perform this task here.

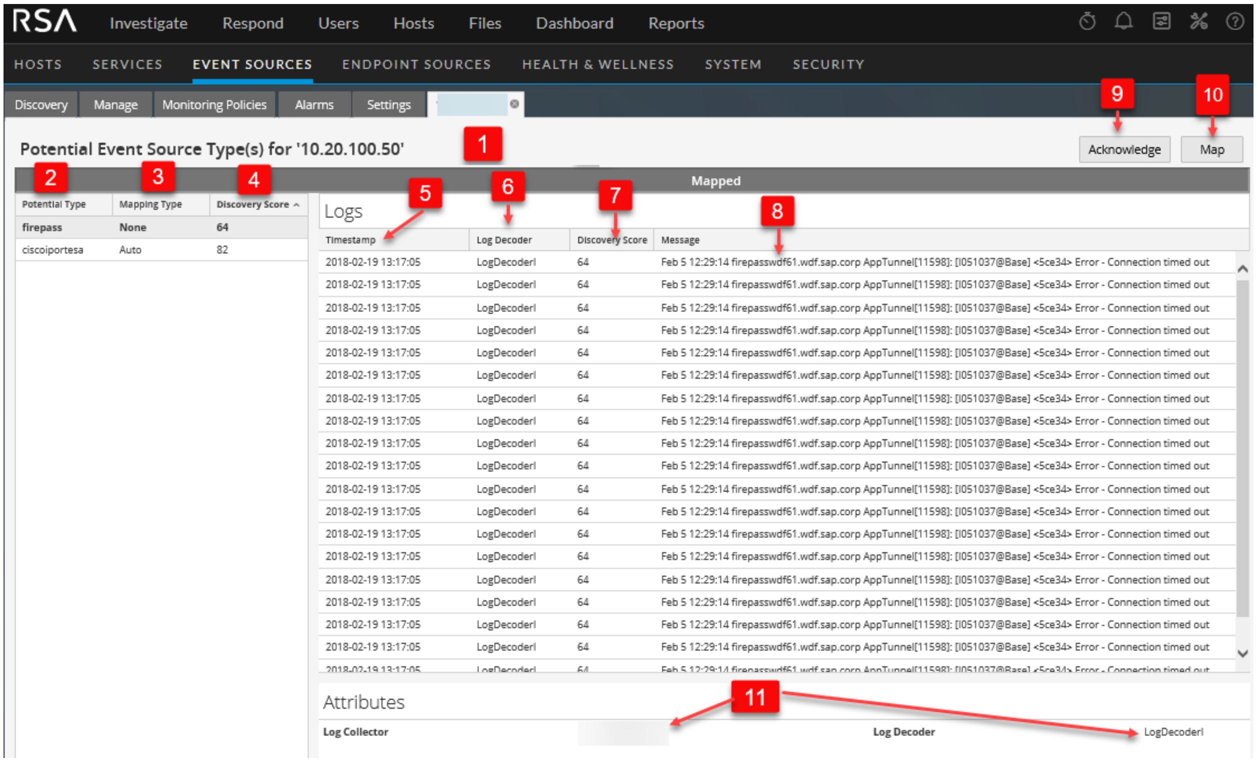
Related Topics

Viewing Logs from Pre-11.0 Log Decoder

Quick Look

The following example shows the discovery scores, event source types, logs, and attributes that correspond with the Event Source you selected in the Event Sources panel for a single Log Decoder.

Note: Device logs are only available for 11.0.0.0 and above Log Decoders.



Potential Event Source Type(s) for '10.20.100.50'

Potential Type	Mapping Type	Discovery Score
firepass	**None**	**64**
ciscoiportesa	Auto	82

Timestamp	Log Decoder	Discovery Score	Message
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out
2018-02-19 13:17:05	LogDecoderl	64	Feb 5 12:29:14 firepasswdf61.wdf.sap.corp AppTunnel[11598]: [I051037@Base] <5ce34> Error - Connection timed out

Log Collector		Log Decoder	LogDecoderl

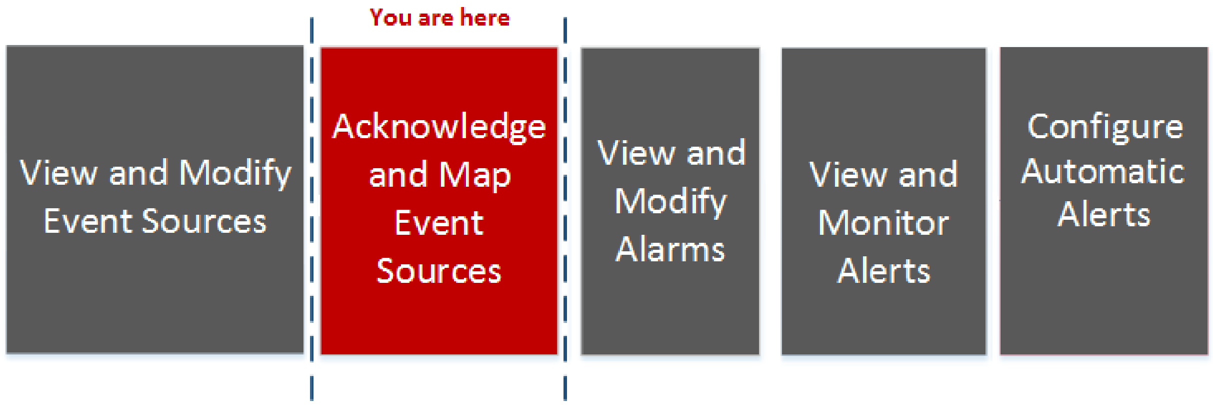
1	Displays the address of the selected Event Source.
2	Displays the potential type of the selected Event Source.
3	Displays the selected Event Source Mapping Type as Auto-Mapped, Manually Mapped, or None. Any changes to the Event Source Mapping are only displayed here.
4	Displays the discovery score for the selected Event Source type from least confident (0) to most confident (100).
5	Displays timestamps for the last few logs that have been parsed to the selected Event Source Type.
6	Displays the address of the Log Decoder that is parsing event sources.
7	Displays the discovery score of the corresponding log.
8	Displays logs for the selected Event Source type.
9	Allows you to acknowledge that all the discovered Event Source types are correct.
10	Allows you to set the appropriate parsers for selected Event Source addresses.
11	Displays the Event Source Management attributes for the selected Event Source Type.

Manage Parser Mappings

The **Manage Parser Mappings** dialog allows you to map the appropriate parsers for selected Event Source addresses. From the **Details** view, select the **Map** button.

Workflow

This workflow shows the overall process for configuring event sources.


You are here
View and Modify Event Sources
Acknowledge and Map Event Sources
View and Modify Alarms
View and Monitor Alerts
Configure Automatic Alerts

What do you want to do?

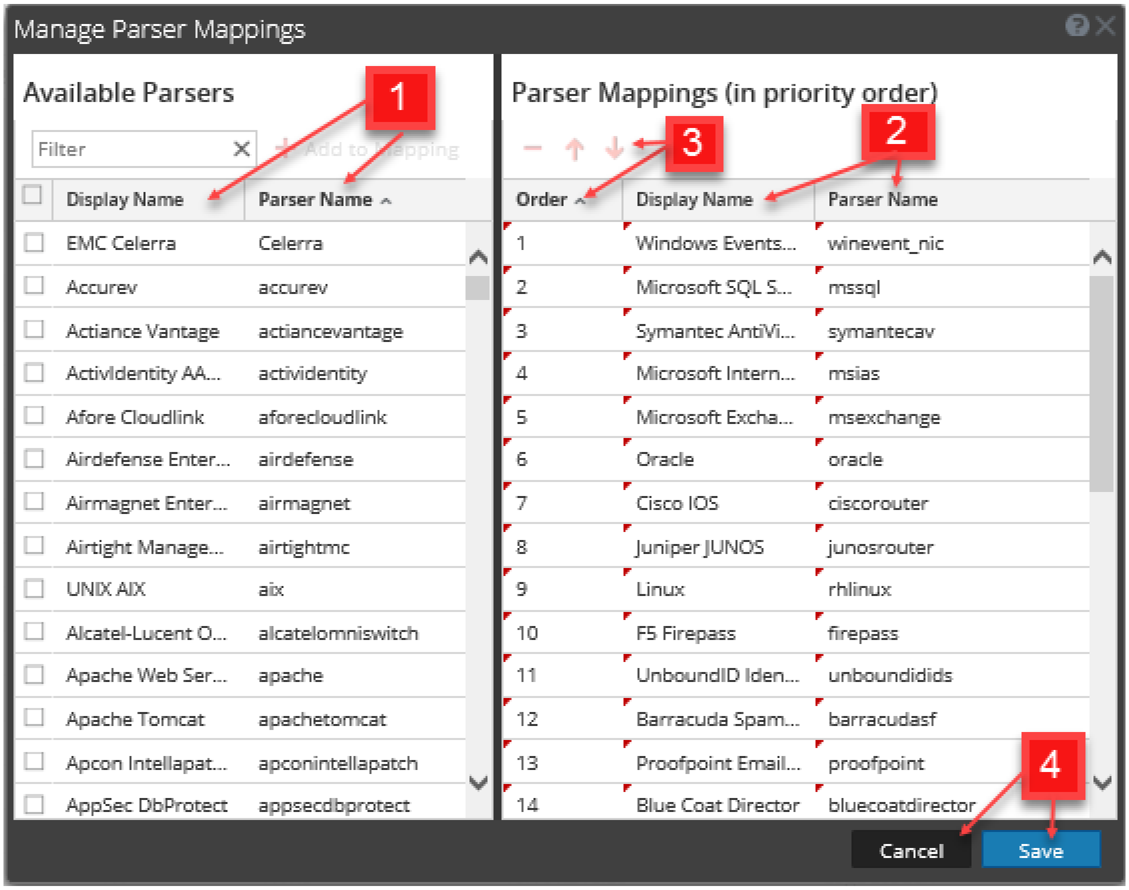
Role	I want to...	Documentation
Administrator	View and modify event sources.	Managing Event Source Groups
Administrator	Acknowledge and map events sources.	Acknowledging and Mapping Event Sources
Administrator	*Add and configure parser mappings for a Log Decoder	Manually Map Event Source Types
Administrator	View event source alarms.	Viewing Event Source Alarms
Administrator	Troubleshoot event source management.	ESM Troubleshooting & Appendix

*You can perform this task here.

Related Topics

Viewing Logs from Pre-11.0 Log Decoder

Quick Look



☐	Display Name	Parser Name
☐	EMC Celerra	Celerra
☐	Accurev	accurev
☐	Actiance Vantage	actiancevantage
☐	ActivIdentity AA...	actividentity
☐	Afore Cloudlink	aforecloudlink
☐	Airdefense Enter...	airdefense
☐	Airmagnet Enter...	airmagnet
☐	Airtight Manage...	airtightmc
☐	UNIX AIX	aix
☐	Alcatel-Lucent O...	alcatelomniswitch
☐	Apache Web Ser...	apache
☐	Apache Tomcat	apachetomcat
☐	Apcon Intellapat...	apconintellapatch
☐	AppSec DbProtect	appsecdbprotect

Order	Display Name	Parser Name
1	Windows Events...	winevent_nic
2	Microsoft SQL S...	mssql
3	Symantec AntiVi...	symantecav
4	Microsoft Intern...	msias
5	Microsoft Excha...	msexchange
6	Oracle	oracle
7	Cisco IOS	ciscorouter
8	Juniper JUNOS	junosrouter
9	Linux	rhlinux
10	F5 Firepass	firepass
11	UnboundID Iden...	unboundidids
12	Barracuda Spam...	barracudasf
13	Proofpoint Email...	proofpoint
14	Blue Coat Director	bluecoatdirector

Note: For event sources that were created manually, the Manage Parser Mappings window has an empty Display Name in the Log Parsers column. To view the missing display names, close the Manage Parser Mappings dialog box, and then reopen it.

1 Displays all the available parsers that you can map based on the event sources that you selected from the **Discovery** view. Also displays the mappings that are already present in the Log Decoders for the selected event source or the parsers that have been discovered.

To filter your available parsers, type the first few letters of the parser name that you want to map. Click the **Add to Mapping** button to add the parser to the parser mappings listed in the right panel.

You need to select parsers before the **Add toMapping** button is enabled.

Add the selected parser by clicking the **Add to Mapping** button in the right panel.

You can rearrange the order of the parser mappings using the up ↑ and down ↓ arrow keys and you can also drag and drop selected parser mappings. You can select multiple mappings by pressing the **Ctrl** key.

2 Displays the names of the selected parsers that you want to map.

3 Displays the order of the selected parser mappings.

You can delete parser mappings by selecting the minus sign (−).
Press the **Ctrl** key to select multiple mappings to perform group operations on them.

4 Click **Save** to save your mappings to all the Log Decoders. A pop-up message informs you that your mappings are successfully saved. When the window is closed, the banner on the **Details** tab is updated to reflect the status. If mapped, the text displayed is **Mapped**.
Click **Cancel** to return to the **Details** tab.

Best Practices

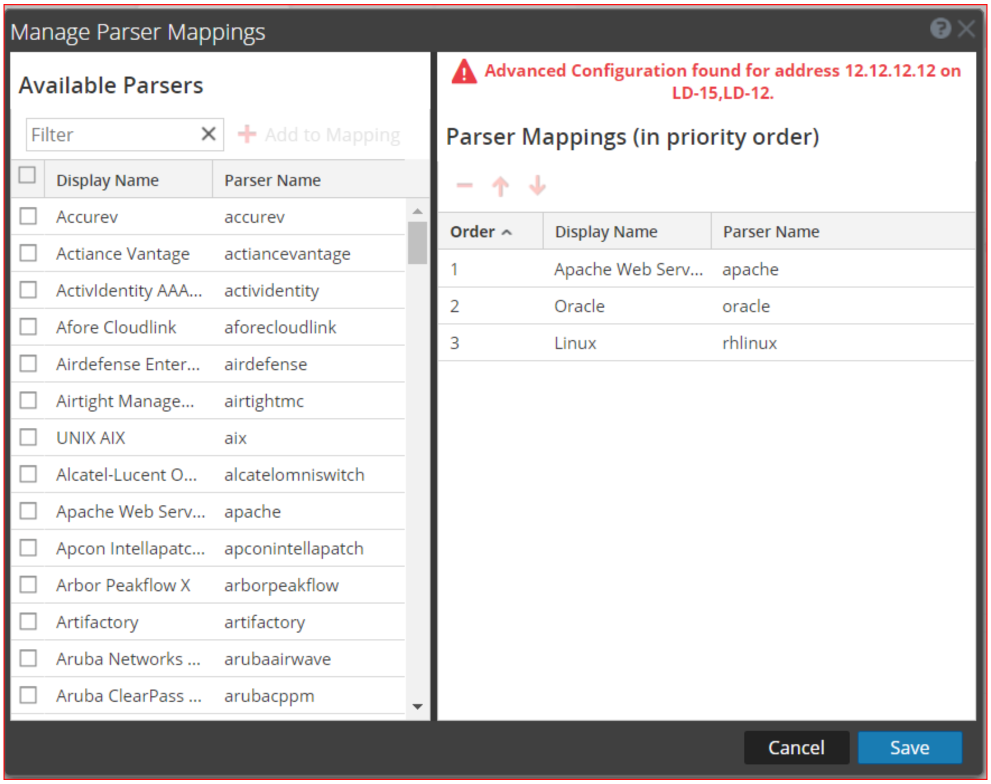
When mapping multiple device types from the same event source, assign the highest priority to the strictest log parser. Conversely, a log parser with generic headers should be lowest in priority. The CEF log parser is an example of a strict log parser.

Advanced Configuration

Mapping configurations with the Log Collector are not displayed in the Parser Mappings window. If the mapping is saved, it is saved for the corresponding IP address, not for the corresponding Log Collector entry. If no mappings are found for the corresponding IP address, the discovered event source types are displayed in the Parser Mappings window.

If advanced Log Decoder configurations are discovered, a message similar to the one below displays in the Manage Parser Mappings dialog.

Note: If you want to edit the advanced configuration, you need to navigate to the Log Decoder service's parser mappings configuration.



Manage Parser Mappings

Available Parsers

Filter ✕ + Add to Mapping

□	Display Name	Parser Name
□	Accurev	accurev
□	Actiance Vantage	actiancevantage
□	ActivIdentity AAA...	activIdentity
□	Afore Cloudlink	aforecloudlink
□	Airdefense Enter...	airdefense
□	Airtight Manage...	airtightmc
□	UNIX AIX	aix
□	Alcatel-Lucent O...	alcatelomniswitch
□	Apache Web Serv...	apache
□	Apcon Intellapatc...	apconintellapatch
□	Arbor Peakflow X	arborpeakflow
□	Artifactory	artifactory
□	Aruba Networks ...	arubaairwave
□	Aruba ClearPass ...	arubacppm

Advanced Configuration found for address 12.12.12.12 on LD-15,LD-12.

Parser Mappings (in priority order)

Order	Display Name	Parser Name
1	Apache Web Serv...	apache
2	Oracle	oracle
3	Linux	rhlinux

Alarms Tab

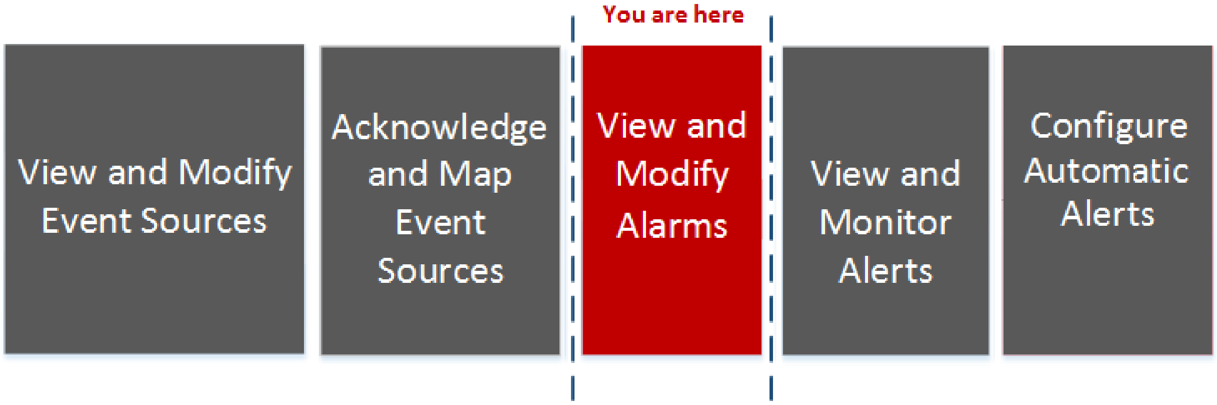
From the Alarms tab you can view details of the alarms that have been generated.

The Alarms tab has one panel that displays Alarm status.

To access this tab, go to (Admin) > **Event Sources** > **Alarms**.

Workflow

This workflow shows the overall process for configuring event sources. It also shows where configuring alarms and alerts settings are located in the process.


You are here
View and Modify Event Sources
Acknowledge and Map Event Sources
View and Modify Alarms
View and Monitor Alerts
Configure Automatic Alerts

What do you want to do?

Role	I want to...	Documentation
Administrator	View and modify event sources.	Managing Event Source Groups
Administrator	Acknowledge and map events sources.	Acknowledging and Mapping Event Sources
Administrator	Add and configure parser mappings for a Log Decoder	Manage Parser Mappings
Administrator	*View event source alarms.	Viewing Event Source Alarms
Administrator	Troubleshoot event source management.	ESM Troubleshooting & Appendix

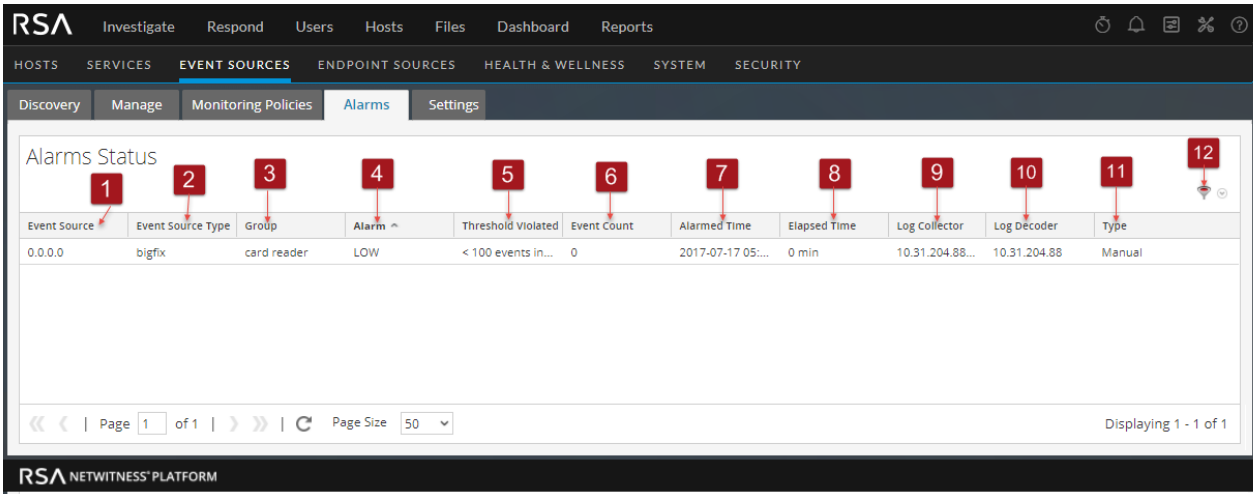
*You can perform this task here.

Related Topics

Configuring Automatic Alerting

Quick Look

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. After the event source returns to a normal state, the corresponding alarm disappears from the list.



Alarms Status

Event Source	Event Source Type	Group	Alarm	Threshold Violated	Event Count	Alarmed Time	Elapsed Time	Log Collector	Log Decoder	Type
0.0.0.0	bigfix	card reader	LOW	< 100 events in...	0	2017-07-17 05:...	0 min	10.31.204.88...	10.31.204.88	Manual

Displaying 1 - 1 of 1

1 Displays the IP, IPv6, or Hostname of the event source that is alarmed.

2 Displays the type of the alarmed event source. For example, **winevent_nic** (for Microsoft Windows) or **rhlinux** (for Linux).

3 Displays the event source group that contains the event source for which the alarm has been triggered.

4 Displays the type of threshold that was triggered: **High** or **Low**

5 Displays the conditions of the threshold that was triggered. For example:

```
5,000,000 events in 5 minutes
```

6 Displays the number of events in the threshold time period causing the alarm.

7 Displays 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).

8 Displays the elapsed time since the event source entered an alarmed state.

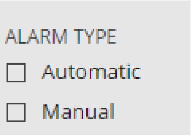
9 Displays the Log Collector last collecting from this event source.

10 Displays the Log Decoder last receiving from this event source.

11 Displays the alarm type. Alarm type is either **Manual** or **Automatic**:

- **Manual**: these are alarms that violate the configured threshold policy.
- **Automatic**: these are alarms that deviate from the baseline for the alarmed event source.

12 Select the **Filter** icon to display the **Filter** menu:



ALARM TYPE
□ Automatic
□ Manual

Select either **Automatic** or **Manual**:

- 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.

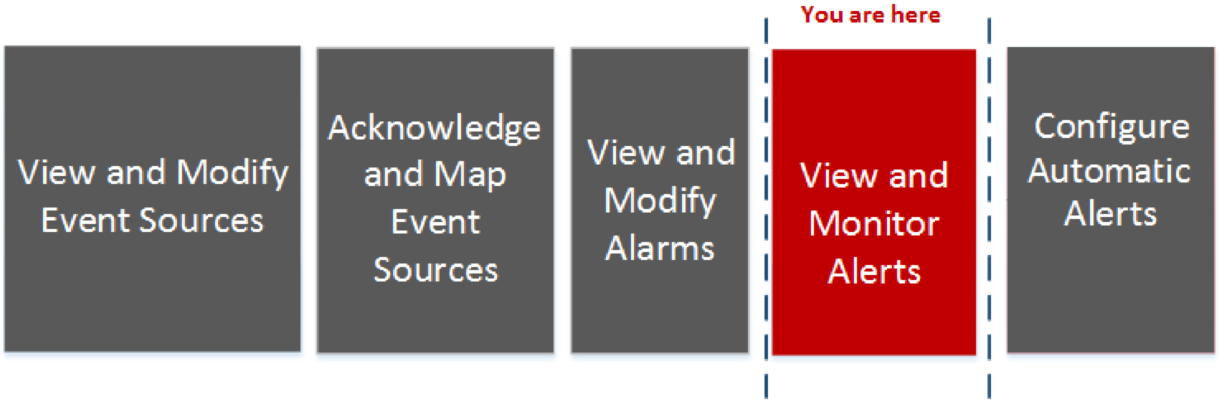
Monitoring Policies Tab

The Monitoring Policies tab organizes thresholds by event source group.

To access this tab, go to (Admin) > **Event Sources** > **Monitoring Policies**.

Workflow

This workflow shows the overall process for configuring event sources.


You are here
View and Modify Event Sources
Acknowledge and Map Event Sources
View and Modify Alarms
View and Monitor Alerts
Configure Automatic Alerts

What do you want to do?

Role	I want to...	Documentation
Administrator	View and modify event sources.	Managing Event Source Groups
Administrator	Acknowledge and map events sources.	Acknowledging and Mapping Event Sources
Administrator	Add and configure parser mappings for a Log Decoder	Manage Parser Mappings
Administrator	View event source alarms.	Viewing Event Source Alarms
Administrator	*View Monitoring Policies.	Monitoring Policies

Role	I want to...	Documentation
Administrator	Troubleshoot event source management.	ESM Troubleshooting & Appendix

*You can perform this task here.

Related Topics

Setting Up Notifications

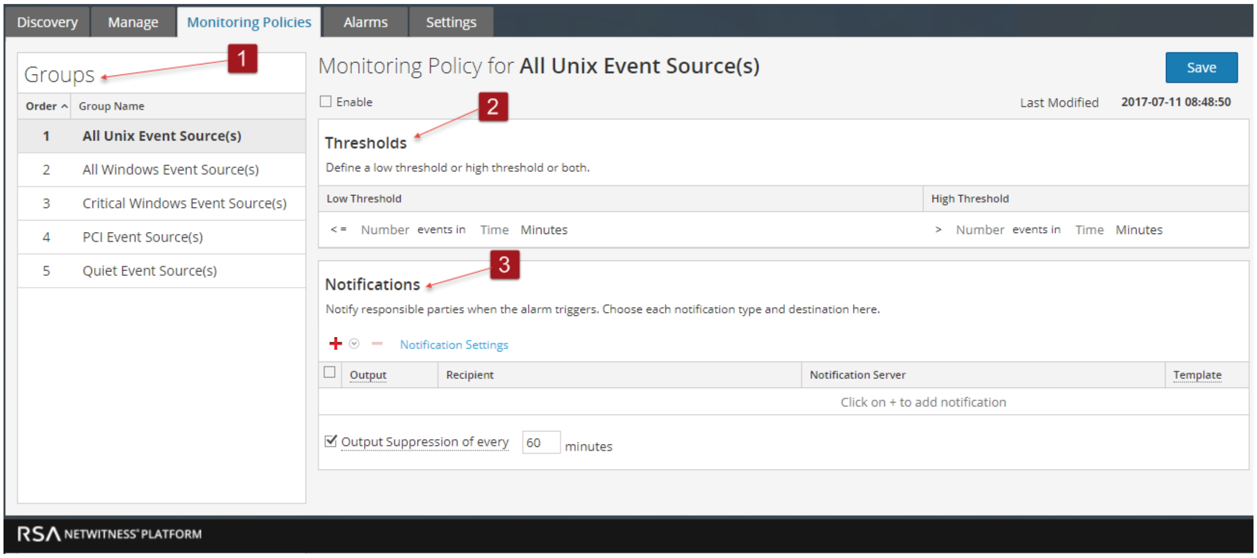
Disabling Notifications

Quick Look

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

- Event Groups Panel
- Thresholds Panel
- Notifications Panel

This is an example of the **Monitoring Policies** tab.



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)

Monitoring Policy for All Unix Event Source(s)

□ Enable

Last Modified 2017-07-11 08:48:50

Thresholds

Define a low threshold or high threshold or both.

Low Threshold	High Threshold
<= Number events in Time Minutes	> Number events in Time Minutes

Notifications

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

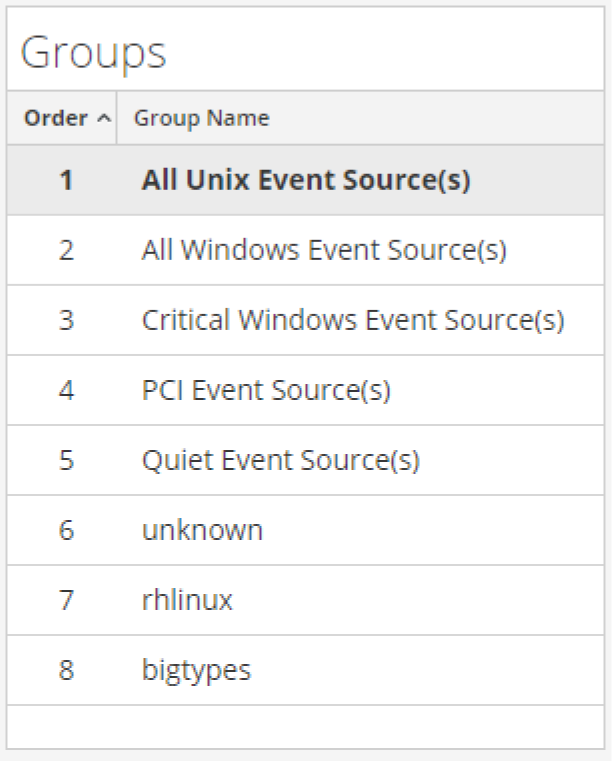
+ − Notification Settings

□	Output	Recipient	Notification Server	Template
Click on + to add notification				

☑ Output Suppression of every 60 minutes

1	Displays the Groups panel.
2	Displays the Thresholds panel.
3	Displays the Notifications panel.

Event Groups Panel



Groups

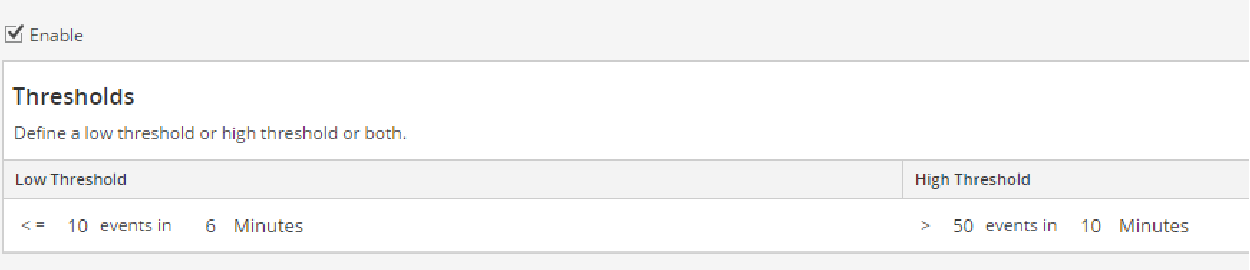
Order ^	Group Name
1	**All Unix Event Source(s)**
2	All Windows Event Source(s)
3	Critical Windows Event Source(s)
4	PCI Event Source(s)
5	Quiet Event Source(s)
6	unknown
7	rhlinux
8	bigtypes

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 NetWitness 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.



☑ Enable

Thresholds

Define a low threshold or high threshold or both.

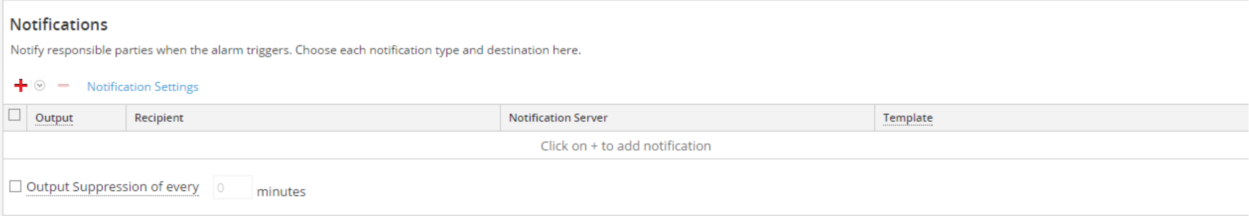
Low Threshold	High Threshold
< = 10 events in 6 Minutes	> 50 events in 10 Minutes

The Thresholds Panel contains the following features.

Feature	Description
Enable	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. **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. 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. See below for more details on the look of notifications.
Low number of events Low number of minutes or hours	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.
High number of events High number of minutes or hours	Works similarly as for the low values: If more messages than specified here are received, the threshold is not met, and notifications are sent.
Last Modified date and time	This field indicates the last time and date that the thresholds were changed.
Save	Saves the changes you have made to the thresholds.

Notifications Panel

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



Notifications

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

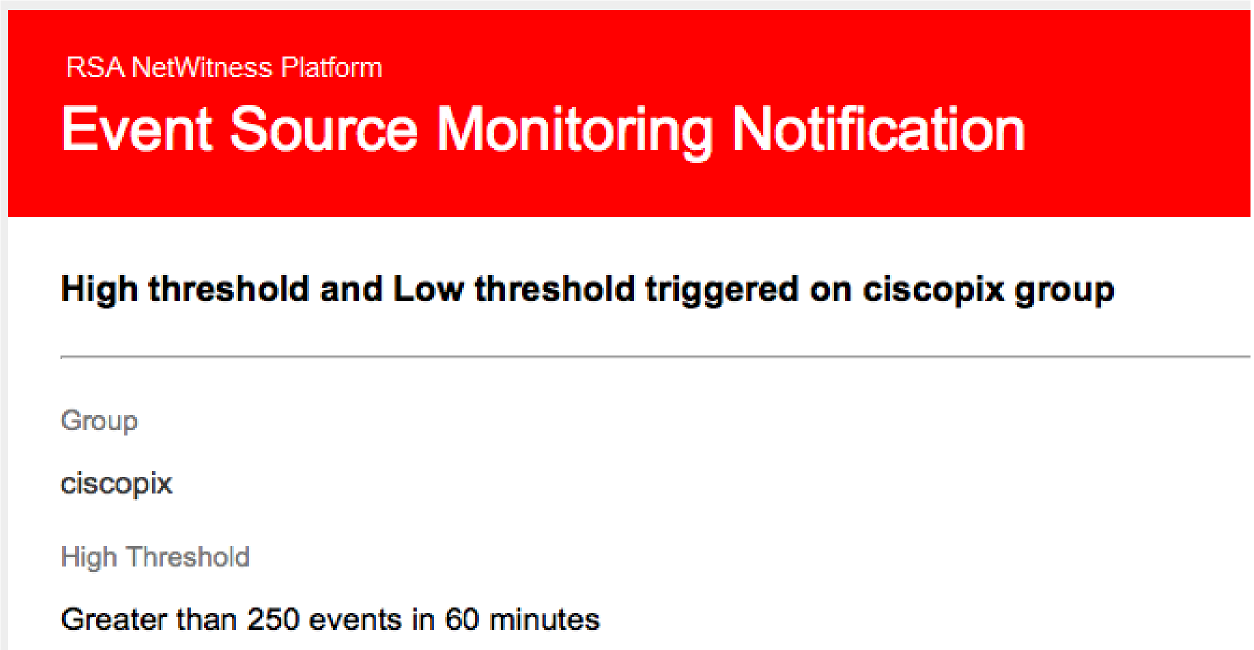
□	Output	Recipient	Notification Server	Template
		Click on + to add notification		

□ Output Suppression of every 0 minutes

The following table describes the fields on the Notifications panel

Field	Description
Tools + -	The following items are available on the toolbar: • **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 NetWitness.
Type	Displays the type of the notification that you have chosen. The available options are as follows: • Email • SNMP • Syslog
Notification	See the **Configure Notification Outputs** topic in the *System Configuration Guide* for more details.
Notification Server	See the **Configure Notification Servers** topic in the *System Configuration Guide* for more details
Template	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: • **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. See the **Configure /Templates for Notifications** topic in the *System Configuration Guide* for more details.
Output Suppression	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.

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



RSA NetWitness Platform

Event Source Monitoring Notification

High threshold and Low threshold triggered on ciscopix group

Group

ciscopix

High Threshold

Greater than 250 events in 60 minutes

- Email:

  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="NetWitness
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:

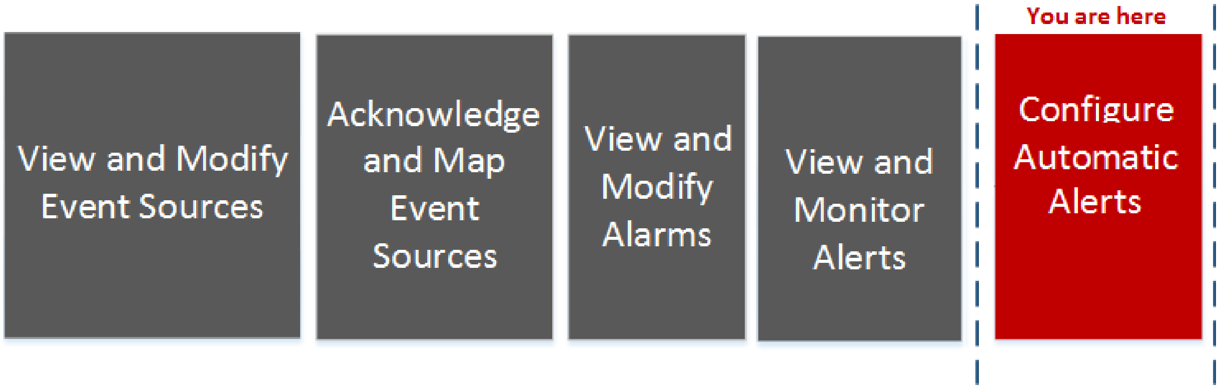
```
11-11-2015 11:57:33 User.Info 127.0.0.1 Nov 11 11:57:33 localhost
CEF:0|RSA|NetWitness Event Source Monitoring|10.6.0.0.0|
HighThresholdAlert|ThresholdExceeded|1|cat=PCI Event Source(s)|Devices|
src=10.17.0.10,ciscopix,Manual|src=10.17.0.13,ciscopix,Manual|src=10.1
7.0.8,ciscopix,Manual|src=10.17.0.8,ciscopix,Automatic|src=10.17.0.12,
ciscopix,Manual|src=10.17.0.5,ciscopix,Manual|src=10.17.0.6,ciscopix,M
anual|src=10.17.0.4,ciscopix,Manual|src=10.17.0.4,ciscopix,Automatic|s
rc=10.17.0.3,ciscopix,Manual|
```

Settings Tab

The Settings tab presents options for automatic monitoring (baseline alerting). To access this tab, go to (Admin) > **Event Sources** > **Settings**.

Workflow

This workflow shows the overall process for configuring event sources.


View and Modify Event Sources
Acknowledge and Map Event Sources
View and Modify Alarms
View and Monitor Alerts
You are here
Configure Automatic Alerts

What do you want to do?

Role	I want to...	Documentation
Administrator	View and modify event sources.	Managing Event Source Groups
Administrator	Acknowledge and map events sources.	Acknowledging and Mapping Event Sources
Administrator	Add and configure parser mappings for a Log Decoder	Manage Parser Mappings
Administrator	View event source alarms.	Viewing Event Source Alarms
Administrator	*Configure Automatic Alerts.	Automatic Alerting

Role	I want to...	Documentation
Administrator	Troubleshoot event source management.	ESM Troubleshooting & Appendix

*You can perform this task here.

Related Topics

Automatic Alerting

Disabling Notifications

Quick Look

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

About Automatic Alerting

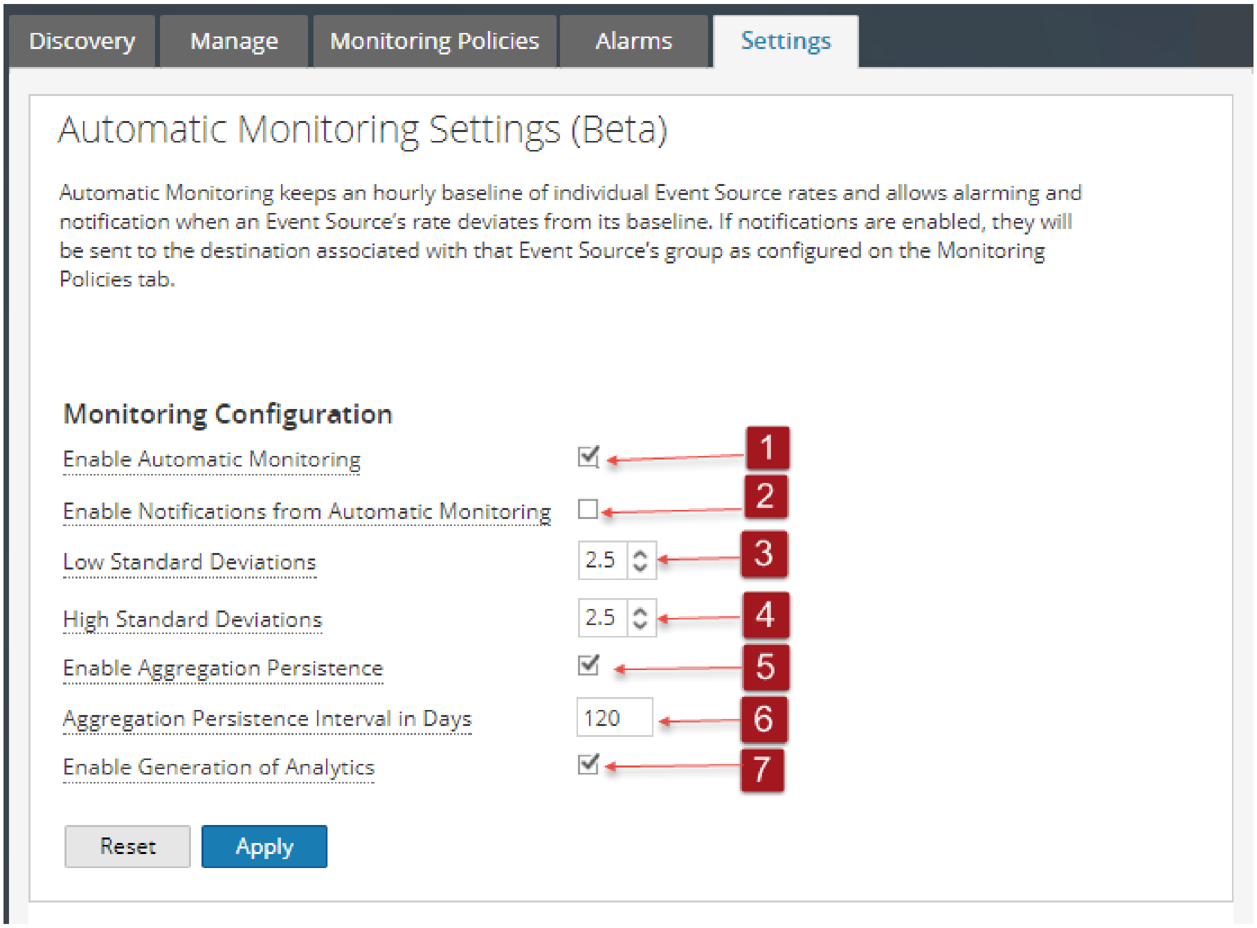
You can set up policies and thresholds for your event source groups. You do this so that you receive notifications when the thresholds are not met. NetWitness also provides an automatic way to receive alarms, if you do not want to set up thresholds to generate alarms.

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:

- After 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.

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



Automatic Monitoring Settings (Beta)

Automatic Monitoring keeps an hourly baseline of individual Event Source rates and allows alarming and notification when an Event Source's rate deviates from its baseline. If notifications are enabled, they will be sent to the destination associated with that Event Source's group as configured on the Monitoring Policies tab.

Monitoring Configuration

Enable Automatic Monitoring ☑

Enable Notifications from Automatic Monitoring □

Low Standard Deviations 2.5

High Standard Deviations 2.5

Enable Aggregation Persistence ☑

Aggregation Persistence Interval in Days 120

Enable Generation of Analytics ☑

1 Determines whether automatic alerting is on or off. By default, this option is selected (automatic alerting turned on)

2 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)

3 The standard deviations below which to receive alerts. Default is **2.5** (95% confidence)

4 The standard deviations above which to receive alerts. Default is **2.5** (95% confidence)

5 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.

- **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

6 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

7 When enabled, data about the behavior of the automatic alerting is stored to disk. The default value is **Enabled**.

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.

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

8 The **Reset** option discards any unsaved changes for all settings on the page.

9 Click **Apply** to save any changes you made to the values on the page.

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 **2.5** (95% confidence)
High Standard Deviations	The standard deviations above which to receive alerts. Default is **2.5** (95% confidence)
Enable Aggregation Persistence	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. • 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	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

Feature	Description
Enable Generation of Analytics	When enabled, data about the behavior of the automatic alerting is stored to disk. The default value is **Enabled**. 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. 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
Reset	This option discards any unsaved changes for all settings on the page.
Apply	Click **Apply** to save any changes you made to the values on the page.

ESM Troubleshooting & Appendix

Troubleshooting Topics:

- Alarms and Notifications Issues
- Duplicate Log Messages
- Troubleshooting Feeds
- Import File Issues
- Negative Policy Numbering

Appendix: Viewing Logs from Pre-11.0 Log Decoder

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 **Settings** tab (🛠 (Admin) > 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 🛠 **(Admin) > 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 🛠 (Admin) **> 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 NetWitness and Log Decoders:

   ```
   service collectd stop
   ```

2. Remove the ESM Aggregator persisted file on NetWitness:

   ```
   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.
5. Start the collectd service:

```
service collectd start
```

Troubleshooting 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 NetWitness.

After 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.

After 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, NetWitness 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","Apachegrp"
     "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 NetWitness Log Decoders at version 10.5 or later? If not, you need to upgrade them. For NetWitness 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
```

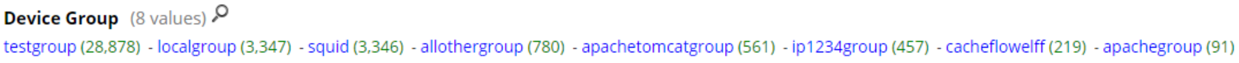
This is a sample logstats file with group information:

```
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.

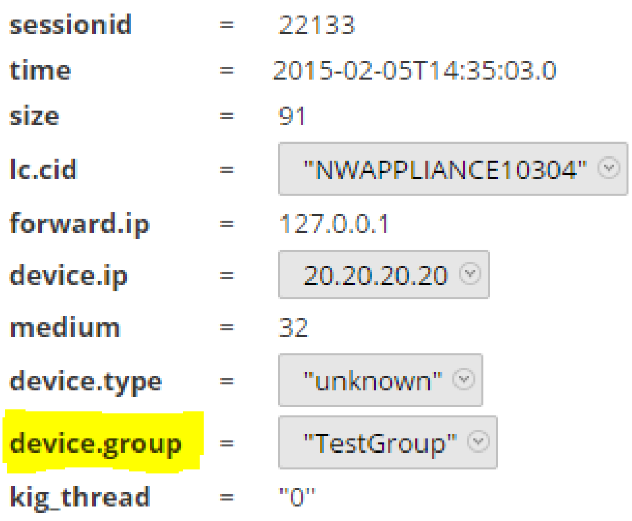
Device Group Meta on Concentrator

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) - cacheflowelff (219) - apachegroup (91)



sessionid = 22133

time = 2015-02-05T14:35:03.0

size = 91

lc.cid = "NWAPPLIANCE10304"

forward.ip = 127.0.0.1

device.ip = 20.20.20.20

medium = 32

device.type = "unknown"

device.group = "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 LogDeocder : <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
al-least on group with at least one eventsource.
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 in **/etc/collectd.d/logdecoder-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   "/etc/pki/nw/node/node-key.pem"
        certpath  "/etc/pki/nw/node/node-cert.pem"
        interval  "600"
        query     "all"
        <stats>
        </stats>
    </Module>
    <Module "NgEsmReader" "update">
        port      "56002"
        ssl       "yes"
        keypath   "/etc/pki/nw/node/node-key.pem"
        certpath  "/etc/pki/nw/node/node-cert.pem"
        interval  "60"
        query     "update"
        <stats>
        </stats>
    </Module>
</Plugin>
```

2. Run the command:

```
collectd service 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 NetWitness, uncomment the verbose flag in **/etc/collectd.d/ESMAggregator.conf**:

   ```
       # ESMAggregator module collectd.conf configuration file
       #
       # Copyright (c) 2014 RSA The Security Divsion 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:

   ```
   collectd service 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: Dispatching
ESM stat NWAPPLIANCE15788/esma_update-cacheflowelff/esm_counter-3.3.3.3 with a
value of 1752 for NWAPPLIANCE15788/cacheflowelff/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 = Cacheflowelff,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: Dispatching
RRD stat NWAPPLIANCE15788/esma_rrd-cacheflowelff/esm_counter-3.3.3.3 with a
value of 1752 for NWAPPLIANCE15788/cacheflowelff/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, an 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:

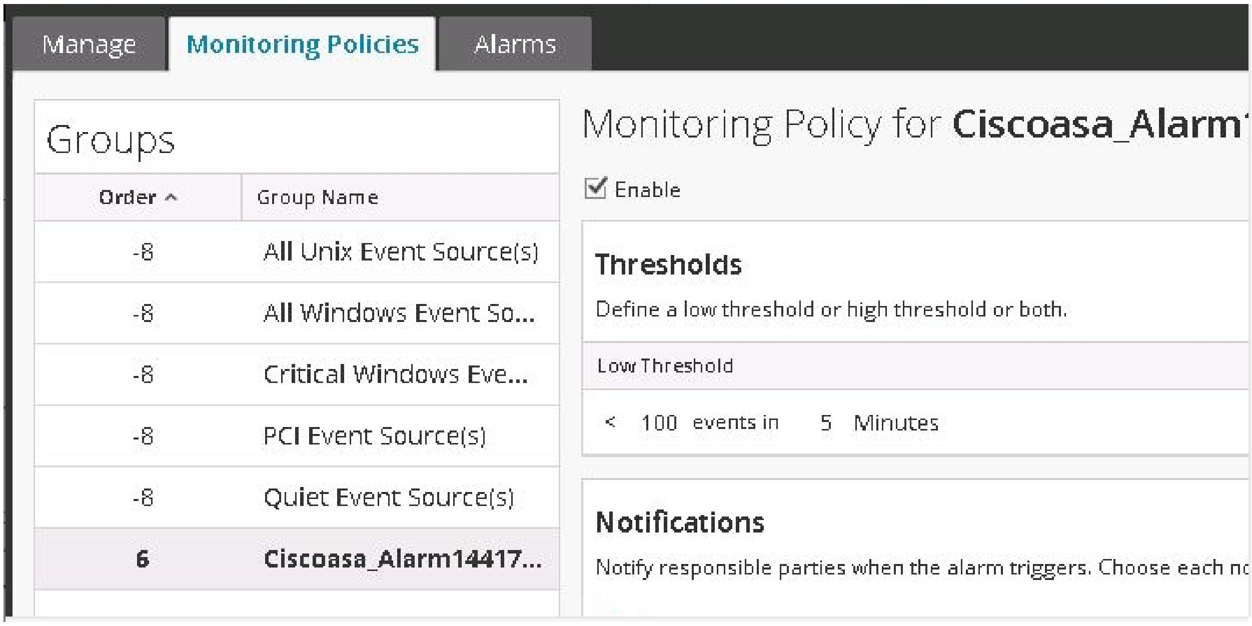
- If you are adding unknown sources, each line in the file must contain a combination of the required attributes:
  - IP or IPv6 or Hostname, and
  - Event Source Type
- The first line of the file must contain header names, and the names must match the names in NetWitness. To get a list of correct column 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 Polices 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.



Groups

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...**

Monitoring Policy for **Ciscoasa_Alarm1**

☑ 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 NetWitness and Log Decoders:

   ```
   Service collectd stop
   ```

2. Remove the ESM Aggregator persisted file on NetWitness:

   ```
   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.

Viewing Logs from Pre-11.0 Log Decoder

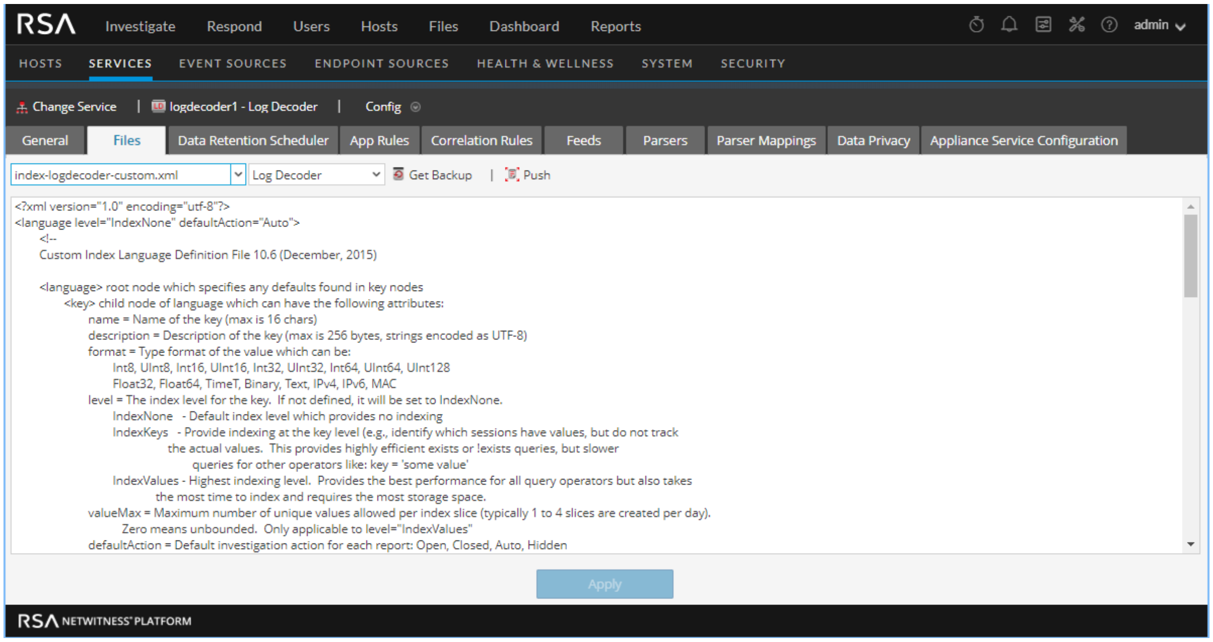
NetWitness 11.0 added the capability to view a small sampling of recent logs for specific devices through detail tabs of the Discovery View. By default, Log Decoders prior to 11.0 do not have the necessary configuration to enable this feature, but a few minor changes can make it available.

To enable logs preview for a pre-11.0.0.0 Log Decoder, follow these steps on the Log Decoder:

1. Go to 🛠 **(Admin) > Services >** select a Log Decoder, then select ⚙ ⌄ **> View > Config**.
2. Click **Files** tab, then select **index-logdecoder-custom.xml** from the drop-down menu.
3. Add the following three lines at the end of the file (before the closing language tag):

   ```
   <key description="Device IP" level="IndexValues" name="device.ip" format="IPv4"
   valueMax="100000" defaultAction="Open"/>
   <key description="Device IPv6" level="IndexValues" name="device.ipv6" format="IPv6"
   valueMax="100000" defaultAction="Open"/>
   <key description="Device Host" level="IndexValues" name="device.host" format="Text"
   valueMax="100000" defaultAction="Open"/>
   ```

4. Click **Apply**.



```
<?xml version="1.0" encoding="utf-8"?>
<language level="IndexNone" defaultAction="Auto">
    <!--
    Custom Index Language Definition File 10.6 (December, 2015)

    <language> root node which specifies any defaults found in key nodes
        <key> child node of language which can have the following attributes:
            name = Name of the key (max is 16 chars)
            description = Description of the key (max is 256 bytes, strings encoded as UTF-8)
            format = Type format of the value which can be:
                Int8, UInt8, Int16, UInt16, Int32, UInt32, Int64, UInt64, UInt128
                Float32, Float64, TimeT, Binary, Text, IPv4, IPv6, MAC
            level = The index level for the key.  If not defined, it will be set to IndexNone.
                IndexNone   - Default index level which provides no indexing
                IndexKeys   - Provide indexing at the key level (e.g., identify which sessions have values, but do not track
                         the actual values.  This provides highly efficient exists or !exists queries, but slower
                             queries for other operators like: key = 'some value'
                IndexValues - Highest indexing level.  Provides the best performance for all query operators but also takes
                       the most time to index and requires the most storage space.
            valueMax = Maximum number of unique values allowed per index slice (typically 1 to 4 slices are created per day).
                  Zero means unbounded.  Only applicable to level="IndexValues"
            defaultAction = Default investigation action for each report: Open, Closed, Auto, Hidden
```

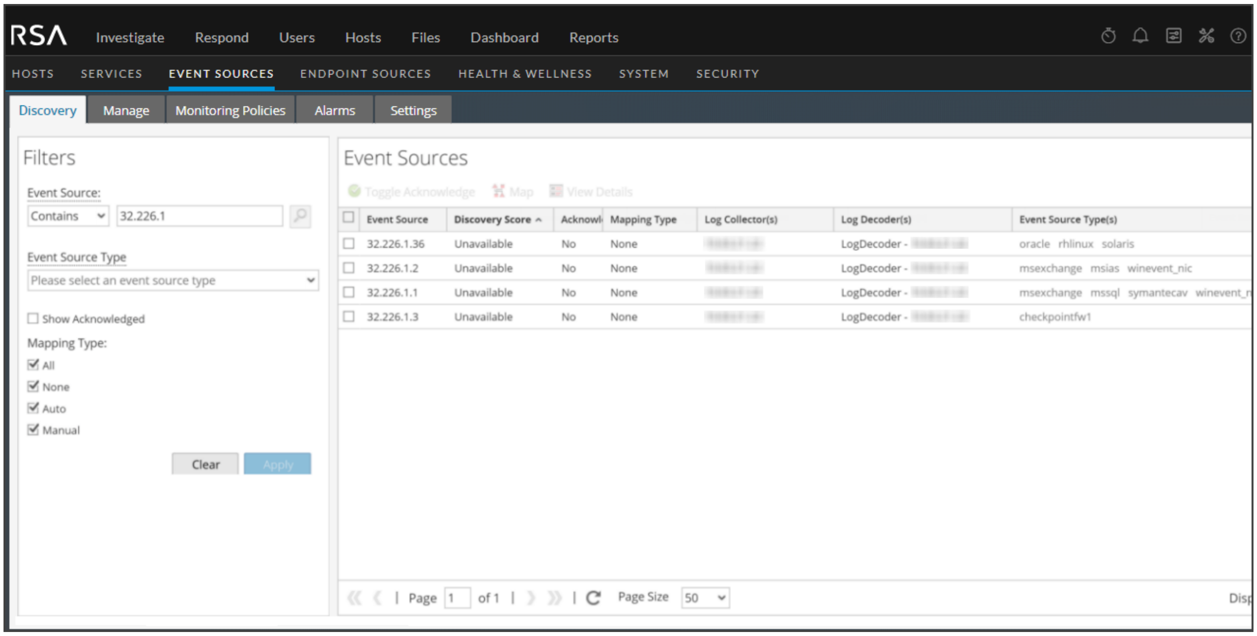
5. Restart the Log Decoder as follows.

   Select **Log Decoder** > **Explore** > **sys** > **Properties** > **shutdown**

This is an example of the **index-logdecoder-custom.xml** file.

Note: Discovery Scores are only available for 11.0 and above Log Decoders. Discovery Scores for pre-11.0 Log Decoders display as Unavailable.

The following example displays the Discovery Score as **Unavailable** in the **Details** view for a pre-11.0 Log Decoder.



Filters

Event Source: Contains 32.226.1

Event Source Type: Please select an event source type

☐ Show Acknowledged

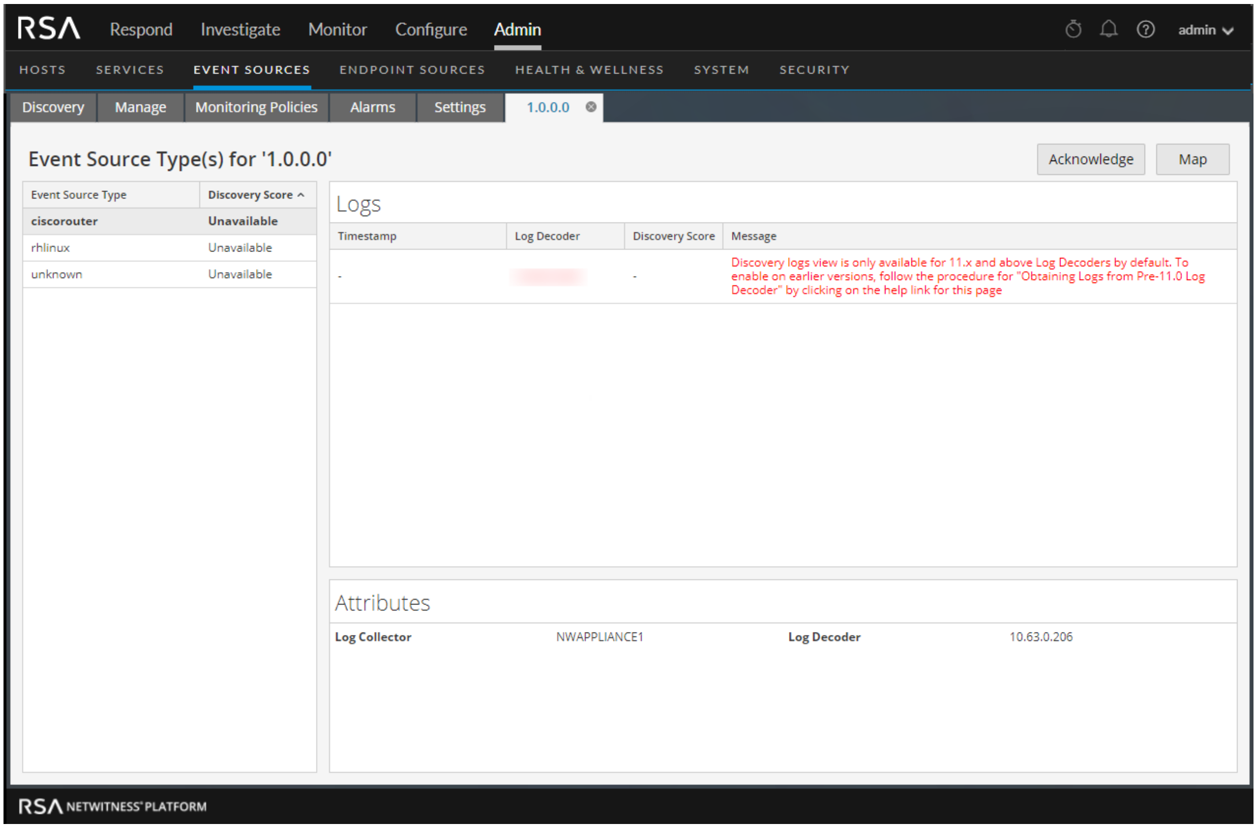
Mapping Type:
☑ All
☑ None
☑ Auto
☑ Manual

Event Sources

☐	Event Source	Discovery Score ^	Acknowl	Mapping Type	Log Collector(s)	Log Decoder(s)	Event Source Type(s)
☐	32.226.1.36	Unavailable	No	None	[redacted]	LogDecoder - [redacted]	oracle rhlinux solaris
☐	32.226.1.2	Unavailable	No	None	[redacted]	LogDecoder - [redacted]	msexchange msias winevent_nic
☐	32.226.1.1	Unavailable	No	None	[redacted]	LogDecoder - [redacted]	msexchange mssql symantecav winevent_r
☐	32.226.1.3	Unavailable	No	None	[redacted]	LogDecoder - [redacted]	checkpointfw1

Note: Device logs are only available for 11.0 and above Log Decoders.

The following example shows the message that displays in the displays in the Logs panel for a pre-11.0 Log Decoder.



Event Source Type(s) for '1.0.0.0'

Event Source Type	Discovery Score
ciscorouter	Unavailable
rhlinux	Unavailable
unknown	Unavailable

Logs

Timestamp	Log Decoder	Discovery Score	Message
-	[redacted]	-	Discovery logs view is only available for 11.x and above Log Decoders by default. To enable on earlier versions, follow the procedure for "Obtaining Logs from Pre-11.0 Log Decoder" by clicking on the help link for this page

Attributes

Log Collector	NWAPPLIANCE1	Log Decoder	10.63.0.206