

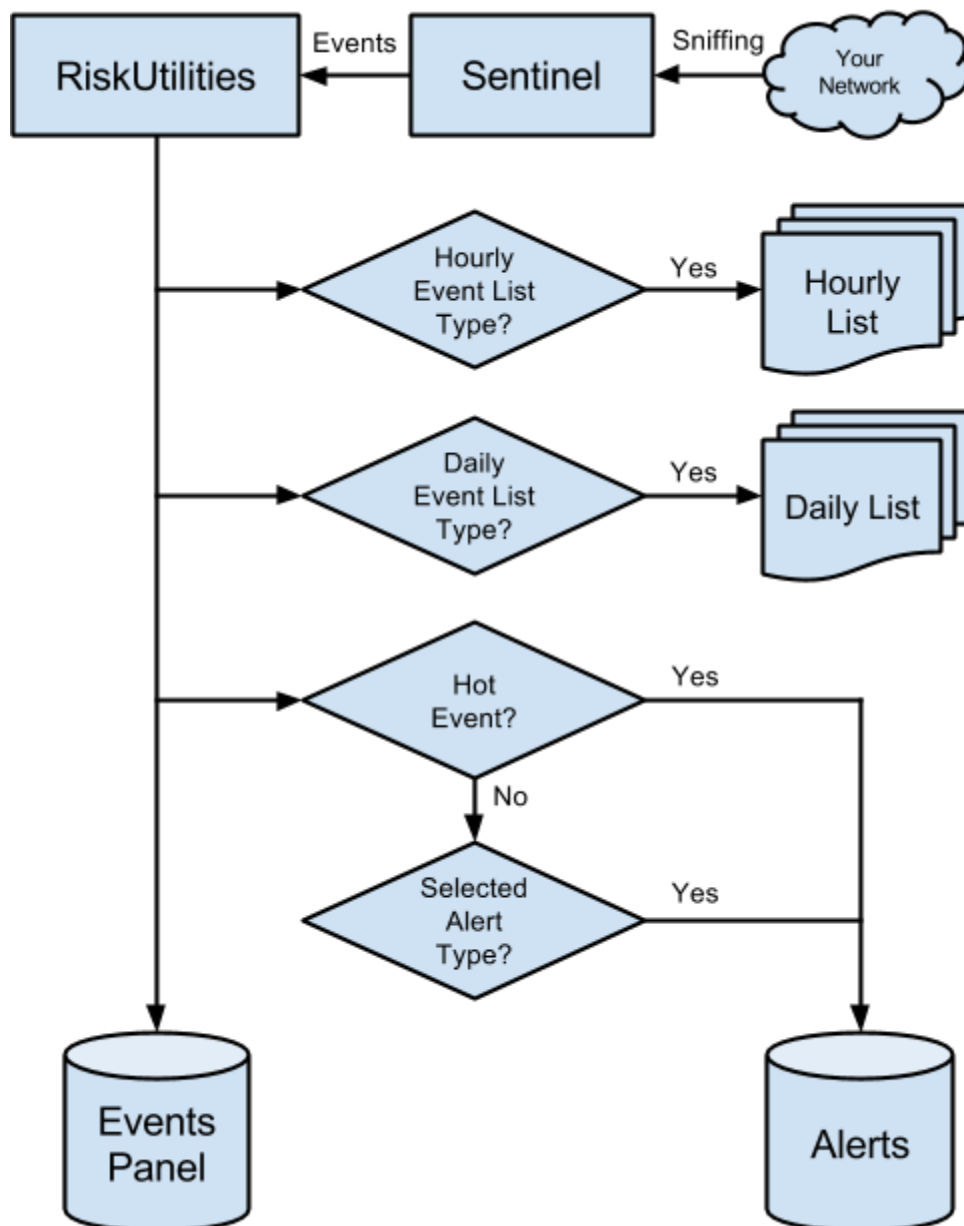
RiskUtilities and Sentinel Alerts

Users Guide

Release 1.0

Events and Alerts

RiskUtilities is the system that works with your Sentinel to keep track of the events that have been seen and tracks the history of the alerts that were generated. RiskUtilities is also used to configure which type of events you are interested in being notified about.



Different Kinds of Notifications

There are four different ways events are tracked in RiskUtilities:

1. **Events Panel** - The events panel shows you a list of all events detected on your network in the last 24-hours. This happens automatically, no configuration is necessary.
2. **Hourly Event List** - You can select types of events you wish to be notified about on an hourly basis. Once an hour, if the selected events have occurred, an email is sent containing a list of the events as well as a copy of the list in CSV format.
3. **Daily Event List** - Works like the Hourly Event List, but is sent out once per day.
4. **Alerts** - Alerts provide a documented workflow to allow you to track the discovery and resolution of security issues on your network. These records are permanently retained for your own reference. You can receive emails when Alerts are created or updated, and choose to receive an SMS messages when a HotAlert, the most serious classification, is created.

Alert Configuration

The Alert Configuration screen can be accessed from the Administration menu in RiskUtilities. It's used to select which types of events trigger the creation of Alerts or are included in the Hourly and Daily Event Lists.

HotAlerts are **always** created from hot events, this setting can not be changed.

Note: These settings are company-wide and apply to all your Sensors.

Alert Configuration

Here you can configure your company wide settings for which kinds of security events trigger instant alerts and which cause periodic emails. To chose whether or not you want to receive one of these emails, click the Profile link in the upper right corner of your screen.

HotAlerts

When an immediate threat is found on your network, we will instantly notify you by sending a HotAlert and creating an alert discussion as soon as we detect any of the issue types you select below.

Send HotAlerts

Alerts

In addition to HotAlerts, we can watch your network for other issues. We will start an alert discussion and send you a message as soon as we detect any of the issue types you select below.

<input checked="" type="checkbox"/> BotNet Command & Control	<input checked="" type="checkbox"/> Equipment Misconfiguration	<input checked="" type="checkbox"/> Internal Malware	<input checked="" type="checkbox"/> P2P Filesharing
<input checked="" type="checkbox"/> Password Exposure	<input checked="" type="checkbox"/> Policy Violation	<input checked="" type="checkbox"/> Server Vulnerability	

Hourly Event List

You can choose to receive an hourly list of events by selecting event types below. Once an hour, we'll send you a message summarizing the events we detected in those categories. No discussions are created for entries on hourly lists unless they are also selected above.

<input checked="" type="checkbox"/> Application Exploit	<input checked="" type="checkbox"/> BotNet Command & Control	<input type="checkbox"/> Brute Force	<input type="checkbox"/> Equipment Misconfiguration
<input type="checkbox"/> External Attack	<input checked="" type="checkbox"/> Internal Malware	<input checked="" type="checkbox"/> Non-Security Event	<input type="checkbox"/> P2P Filesharing
<input type="checkbox"/> Password Exposure	<input type="checkbox"/> Pentester Tools	<input checked="" type="checkbox"/> Policy Violation	<input type="checkbox"/> Proxy Bot
<input type="checkbox"/> RBN CrimeWare	<input type="checkbox"/> Recon Bot	<input type="checkbox"/> Server Vulnerability	<input type="checkbox"/> Spam Bot

Daily Event List

The daily event list works like the hourly list, but we send it out every morning.

<input checked="" type="checkbox"/> Application Exploit	<input checked="" type="checkbox"/> BotNet Command & Control	<input checked="" type="checkbox"/> Brute Force	<input checked="" type="checkbox"/> Equipment Misconfiguration
<input checked="" type="checkbox"/> External Attack	<input checked="" type="checkbox"/> Internal Malware	<input checked="" type="checkbox"/> Non-Security Event	<input checked="" type="checkbox"/> P2P Filesharing
<input checked="" type="checkbox"/> Password Exposure	<input checked="" type="checkbox"/> Pentester Tools	<input checked="" type="checkbox"/> Policy Violation	<input checked="" type="checkbox"/> Proxy Bot
<input checked="" type="checkbox"/> RBN CrimeWare	<input checked="" type="checkbox"/> Recon Bot	<input checked="" type="checkbox"/> Server Vulnerability	<input checked="" type="checkbox"/> Spam Bot

or

Your Profile

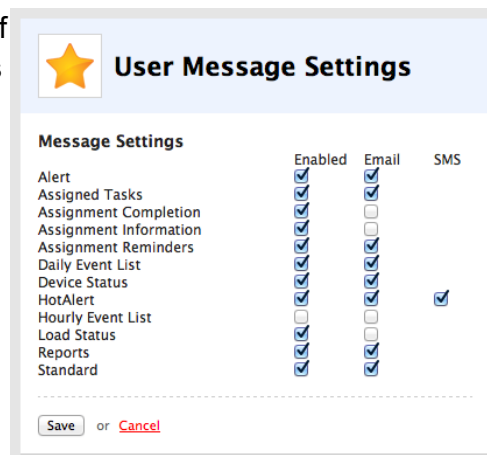
This is the screen you can use to change your email address or phone number. To receive messages from the system your user's Profile must be setup correctly. To access your profile, click the Profile link next to the Logout link on the top-right of the screen.

Note: Multiple users can not share the same email address or SMS number.

User Message Settings

From your Profile, you can click the link on the right side of the screen labeled User Message Settings. Each user has their own personal message settings.

Each type of message the system may send is listed, along with checkboxes to select how they should be handled for your user. This allows you to choose to receive emails when HotAlerts are generated, not regular Alerts.



Message Settings	Enabled	Email	SMS
Alert	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Assigned Tasks	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Assignment Completion	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Assignment Information	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Assignment Reminders	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Daily Event List	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Device Status	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
HotAlert	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Hourly Event List	<input type="checkbox"/>	<input type="checkbox"/>	
Load Status	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Reports	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Standard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

- **Enabled** - The system will generate these messages, and they will show up in the Inbox section of the site. If disabled, you can't receive emails or SMSes.
- **Email** - When selected, not only will the message show up in the Inbox section of the website, but an email message will also be sent to your email address.
- **SMS** - Only available for HotAlerts, when selected we'll send an SMS message to your phone when a new HotAlert is created.

Note: For your convenience, the system will automatically limit the number of messages sent to you. We will not send more than 1 SMS message every 30-minutes. We also apply higher limits to the number of emails from any single type to prevent you from being inundated.

Alert Workflow

Creation

There are two ways Alerts are created in the system. The most common way is for an event matching your Alert Configuration to be detected. When that happens, an Alert will be created automatically. It is also possible for one of RiskAnalytics security professionals to create an alert manually, but this is relatively rare. All Alerts are assigned sequential ID numbers to make them easier to refer to and discuss.

Coalescing

If an event re-occurs while its Alert is still open it will be added to the existing Alert as a recurrence. These can be found in the second tab when viewing an Alert. The tab lists the number of times we've detected the event.



Alert #3416 Discussion

Discussion [Recurrences \(34\)](#)

Subject
External Attack - ATTACK-RESPONSES 403 Forbidden (variant 1)

First Occurrence
June 14, 2013 4:26 AM CDT

Working With Alerts

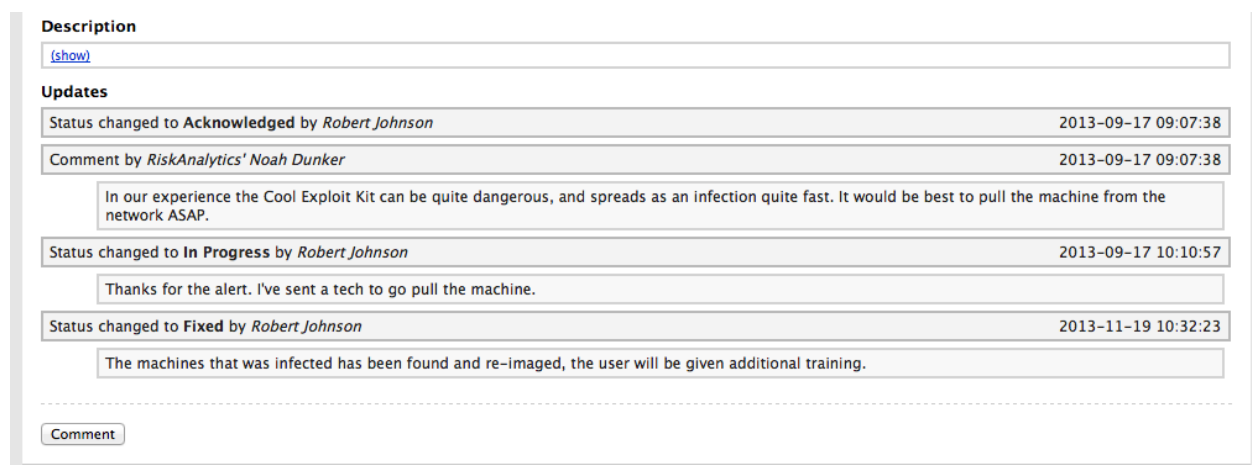
Alerts work like tickets in a ticketing system with five possible statuses. All data related to an Alert is preserved. Even after it has been closed, it's still possible to go back and see the discussion and the status changes the Alert went through. The five possible statuses are:

1. **New** - All Alerts are created with the New status. This indicates that the Alert has never been looked at.
2. **Acknowledged** - Once you've seen an Alert, you should change it to Acknowledged. This indicates that you know the event has occurred, but may not be taking direct action yet.
3. **In-Progress** - This status is designed to indicate that you are actively investigating or working on an Alert.
4. **Fixed** - Closes an Alert and indicates that the issue has been corrected.
5. **Not an Issue** - Also closes an Alert, indicating the issue was a false-positive or is otherwise acceptable.

Note: Low priority Alerts that are Acknowledged and haven't had any activity in 30 days will be closed automatically with a system-generated comment to that effect.

Commenting & Changing Statuses

An Alert's status can only be moved forward. Once an alert has been marked as In-Progress, it can not be changed back to New or Acknowledged. With the exception of marking an Alert as Acknowledged, you have to provide a comment when changing an Alert's status. You can continue to comment on an Alert after it has been closed.



The screenshot shows a user interface for an alert. At the top, there is a 'Description' section with a '(show)' link. Below that is an 'Updates' section containing a list of status changes and comments. The updates are as follows:

Update	Timestamp
Status changed to Acknowledged by <i>Robert Johnson</i>	2013-09-17 09:07:38
Comment by <i>RiskAnalytics' Noah Dunker</i>	2013-09-17 09:07:38
In our experience the Cool Exploit Kit can be quite dangerous, and spreads as an infection quite fast. It would be best to pull the machine from the network ASAP.	
Status changed to In Progress by <i>Robert Johnson</i>	2013-09-17 10:10:57
Thanks for the alert. I've sent a tech to go pull the machine.	
Status changed to Fixed by <i>Robert Johnson</i>	2013-11-19 10:32:23
The machines that was infected has been found and re-imaged, the user will be given additional training.	

At the bottom of the updates section, there is a 'Comment' button.

Tip: If you're setup to get SMS messages when HotAlerts are generated, you can reply to the message with either "ack" or "acknowledge" to quickly mark the Alert as acknowledged.

There are three places where you can interact with Alerts:

1. The Alerts pane on the dashboard lets you quickly change an Alert's status by clicking on the current status.
2. The Alert List has checkboxes next to each Alert. By selecting Alerts and using the buttons below the list you can quickly comment on or change the status of up to 500 Alerts at once. The comments on the Alerts will reflect that the change was part of a bulk operation.
3. When viewing an Alert there are buttons to comment or change the status below the discussion.

Notification of Changes

Whenever a comment is made on an Alert, including when its status is changed, you'll receive an email. This makes it easy to follow the discussion on an Alert so you don't have to keep checking back manually. You can choose to stop being notified about an individual Alert by clicking the link at the bottom of one of the emails.

Reports

Since RiskUtilities permanently tracks each Alert and all its updates, we're able to provide you with two reports to make it easy to assess your security procedures over time.

- **Closed Alerts** - Lists every Alert in the selected date range that was closed by marking as Fixed or Not an Issue. It works as an audit log of all the events your Sentinel is configured to create Alerts for. The report gives you a CSV with the following columns:
 - Alert ID
 - Severity
 - Sensor
 - Open Date
 - Subject
 - Acknowledge Date
 - Acknowledging User
 - Final Status
 - Closed Date
 - Closing User
- **Still-Open Alerts** - Provides a list of Alerts that were created in the selected date range but have not been closed yet. You can use this to find Alerts that have been open a long time and ensure they don't fall through the cracks.