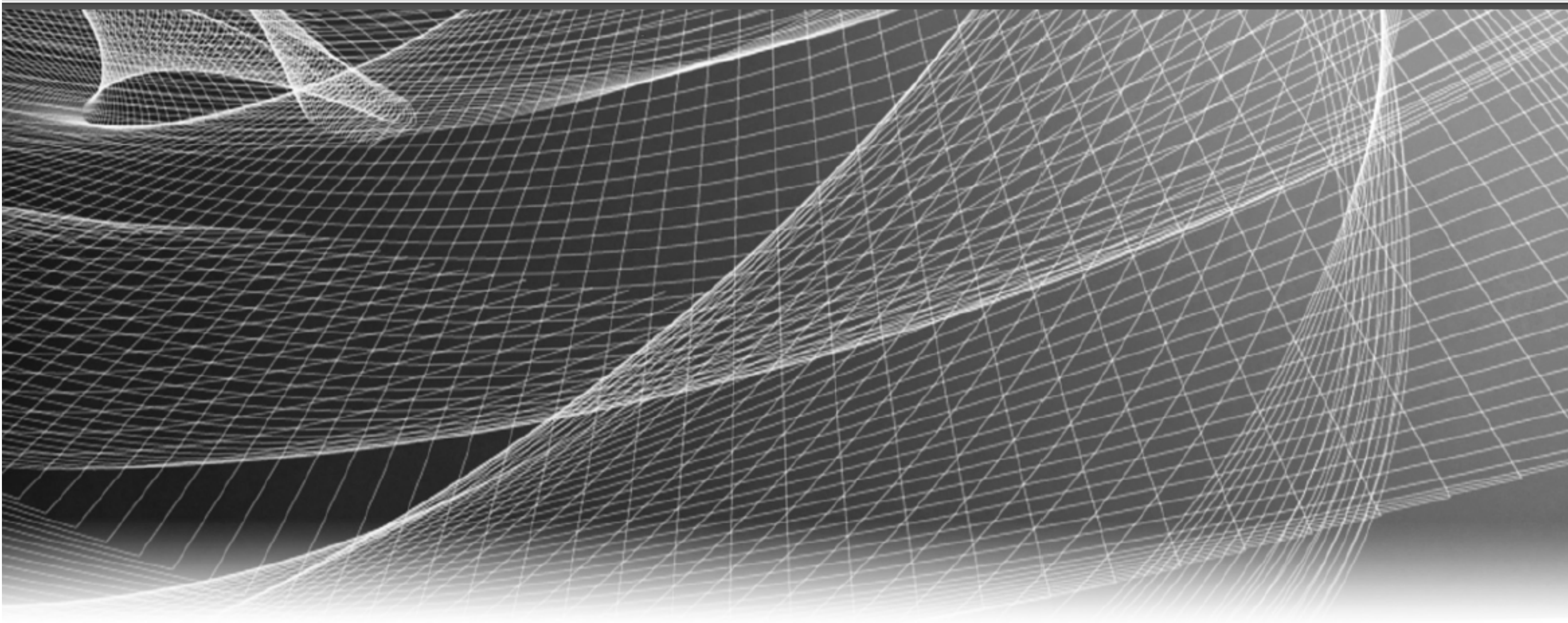


RSA Security Analytics

Incident Management Guide

for Version 10.6.5

Contact Information

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

Trademarks

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

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

October 2017

Contents

Incident Management

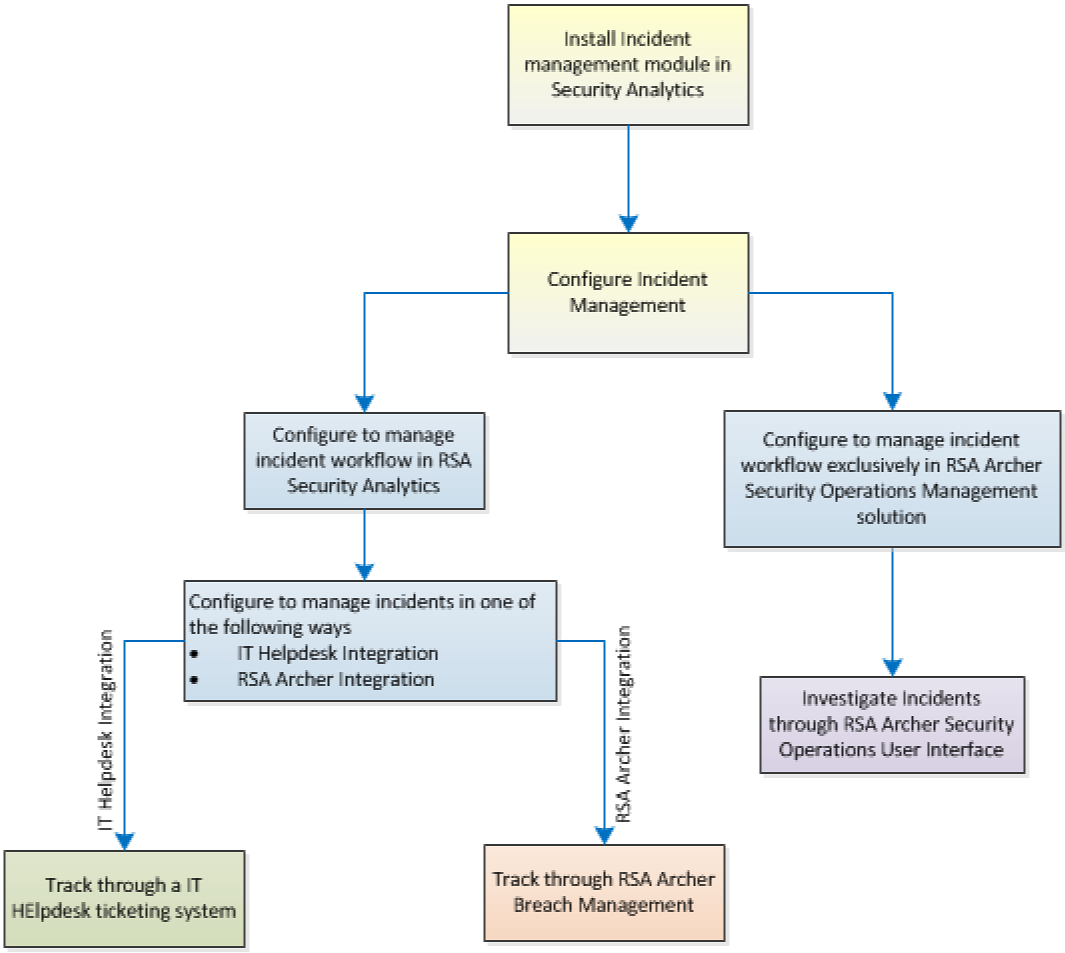
The Incidents module in Security Analytics provides an easy way to track the incident response process. The Incident management solution provides the following:

- Track the Incident Response in a consistent way.
- Automate the process of creating actionable security incidents from incoming alerts.
- Provide business context and investigational tools to help the team discover the root causes.
- Track the remediation process in an automated way by integrating with a third party help desk system.

Most of the investigations are achieved within the Security Analytics interface wherein you can create and track remediation tasks, but Security Analytics also has the following options:

- Integration with a third party ticketing system that enables you to escalate remediation tasks for the Operations target queue as tickets.
- Integration with RSA Archer that enables you to escalate remediation tasks for the **GRC** target queue as Findings or to report data breaches and trigger the breach response process in the RSA Archer Security Operations Management solution.

The following figure depicts various ways in which you can track the incoming alerts and accomplish the incident management process.


Install Incident management module in Security Analytics
Configure Incident Management
Configure to manage incident workflow in RSA Security Analytics
Configure to manage incident workflow exclusively in RSA Archer Security Operations Management solution
Configure to manage incidents in one of the following ways
• IT Helpdesk Integration
• RSA Archer Integration
Investigate Incidents through RSA Archer Security Operations User Interface
IT Helpdesk Integration
RSA Archer Integration
Track through a IT HElpdesk ticketing system
Track through RSA Archer Breach Management

Topics

- Incident Management Process
- Review Alerts
- Incident Management Process Flow
- Automate the Incident Management Process
- System Integration
- Incident Management Reference Information

Incident Management Process

Incident Management Workflow

Security Analytics Incidents module collects alerts from multiple sources and provides the ability to group them logically and start an Incident response workflow to investigate and remediate the security issues raised. Security Analytics Incidents module allows you to configure rules to automate the aggregation of Alerts into Incidents. Alerts will be normalized by the system to a common format to provide users with a consistent view for the rule criteria regardless of the data source. You can build query criteria based on the alert data with the ability to query on fields that are common as well as specific to data sources.

The rule engine allows you to group similar alerts together into an Incident so that the investigation and remediation workflow can be shared across a set of similar alerts. You can create rules that can group alerts into incidents depending on a common value they share for one or two attributes (for example, source hostname) or if they are reported within a limited time window (for example, alerts that are within 4 hours of each other).

If an alert matches a rule, an incident is created using the criteria. As new alerts are ingested, if an existing Incident was already created that matched those criteria, and that incident isn't "in progress" yet, the new alerts will continue to be added to the same incident. If there is no existing incident for the grouped value (for example, the specific hostname) or the time window, a new incident will be created and the alert will be added to it.

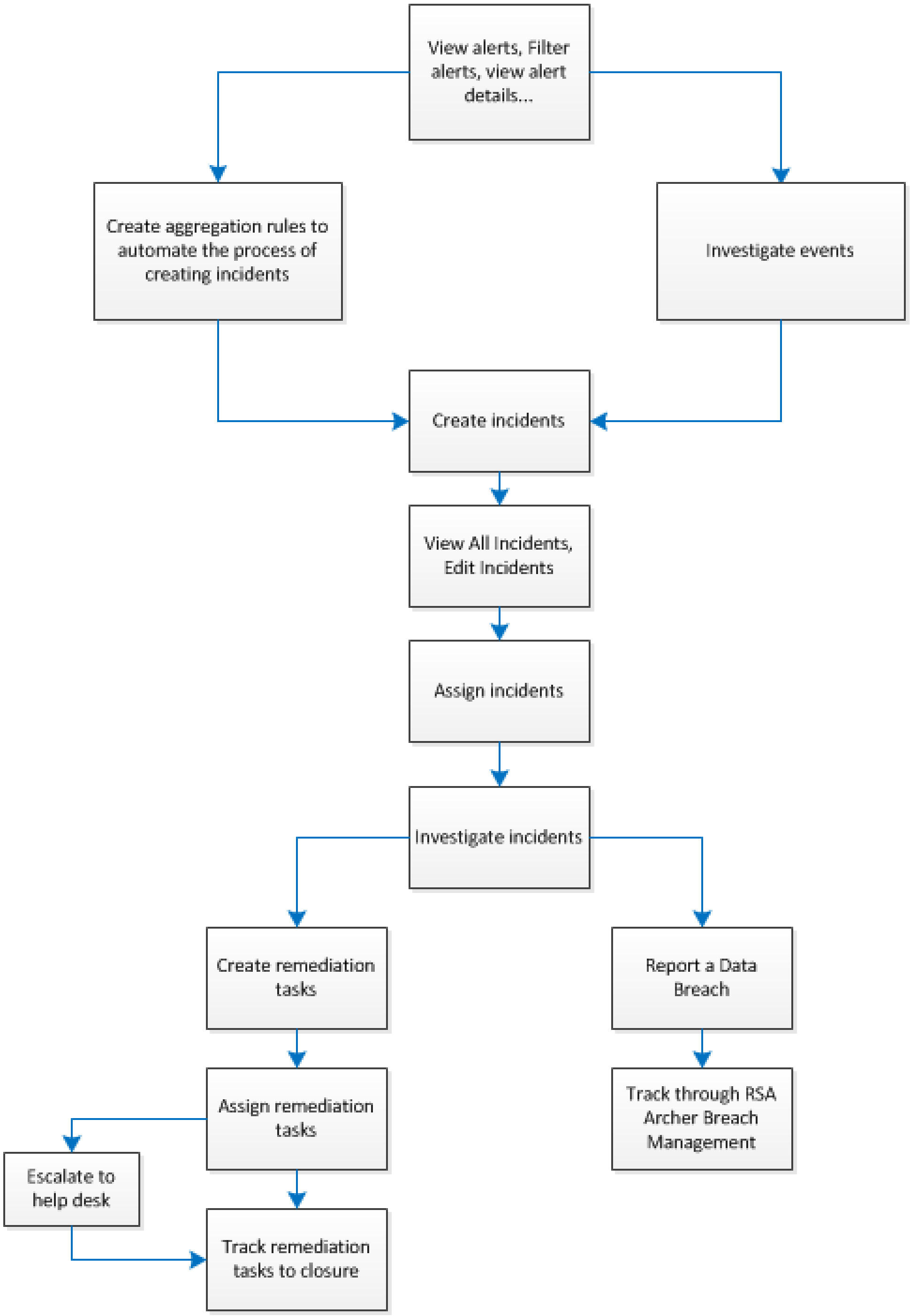
You can have multiple aggregation rules. The rules can either group alerts into Incidents or suppress alerts from being matched by any rule, hence the rules are ranked top-to-bottom and only the first rule to match an incoming alert is be used to include that alert in an incident. The Incidents provide a context for the alerts, provide tools to record the investigation status, and track the remediation progress.

Various stages in the Incident Management process are:

- Review Alerts
- Manage Incidents
- Automate Incident Management process
- Track the incident response through
  - Security Analytics UI
  - a third party helpdesk system
  - RSA Archer Breach management

Incident Management Workflow Diagram

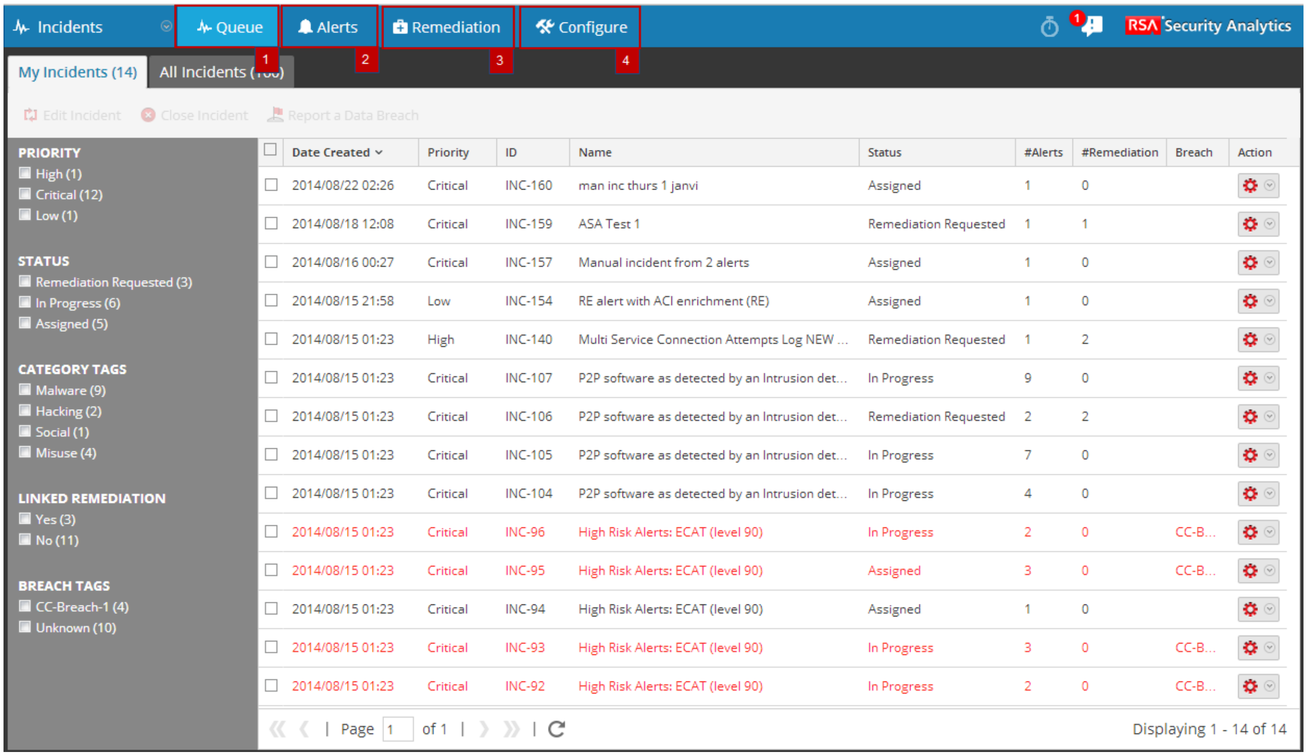
The following figure shows the incident management workflow process.


View alerts, Filter alerts, view alert details...
Create aggregation rules to automate the process of creating incidents
Investigate events
Create incidents
View All Incidents, Edit Incidents
Assign incidents
Investigate incidents
Create remediation tasks
Report a Data Breach
Assign remediation tasks
Track through RSA Archer Breach Management
Escalate to help desk
Track remediation tasks to closure

The Incident Management View

In **Security Analytics** menu, select **Dashboard** > **Incidents**. The various sections of the Incidents module are displayed.

The following figure depicts the Incidents module displayed in the Security Analytics user interface.



PRIORITY
- High (1)
- Critical (12)
- Low (1)

STATUS
- Remediation Requested (3)
- In Progress (6)
- Assigned (5)

CATEGORY TAGS
- Malware (9)
- Hacking (2)
- Social (1)
- Misuse (4)

LINKED REMEDIATION
- Yes (3)
- No (11)

BREACH TAGS
- CC-Breach-1 (4)
- Unknown (10)

□	Date Created	Priority	ID	Name	Status	#Alerts	#Remediation	Breach	Action
□	2014/08/22 02:26	Critical	INC-160	man inc thurs 1 janvi	Assigned	1	0		
□	2014/08/18 12:08	Critical	INC-159	ASA Test 1	Remediation Requested	1	1		
□	2014/08/16 00:27	Critical	INC-157	Manual incident from 2 alerts	Assigned	1	0		
□	2014/08/15 21:58	Low	INC-154	RE alert with ACI enrichment (RE)	Assigned	1	0		
□	2014/08/15 01:23	High	INC-140	Multi Service Connection Attempts Log NEW ...	Remediation Requested	1	2		
□	2014/08/15 01:23	Critical	INC-107	P2P software as detected by an Intrusion det...	In Progress	9	0		
□	2014/08/15 01:23	Critical	INC-106	P2P software as detected by an Intrusion det...	Remediation Requested	2	2		
□	2014/08/15 01:23	Critical	INC-105	P2P software as detected by an Intrusion det...	In Progress	7	0		
□	2014/08/15 01:23	Critical	INC-104	P2P software as detected by an Intrusion det...	In Progress	4	0		
□	2014/08/15 01:23	Critical	INC-96	High Risk Alerts: ECAT (level 90)	In Progress	2	0	CC-B...	
□	2014/08/15 01:23	Critical	INC-95	High Risk Alerts: ECAT (level 90)	Assigned	3	0	CC-B...	
□	2014/08/15 01:23	Critical	INC-94	High Risk Alerts: ECAT (level 90)	Assigned	1	0		
□	2014/08/15 01:23	Critical	INC-93	High Risk Alerts: ECAT (level 90)	In Progress	3	0	CC-B...	
□	2014/08/15 01:23	Critical	INC-92	High Risk Alerts: ECAT (level 90)	In Progress	2	0	CC-B...	

Displaying 1 - 14 of 14

1. **Queue** - In the Incident Queue you can see a list of all incidents assigned and unassigned. You can filter incidents, view incident details, investigate incidents, and track them to closure.
2. **Alerts** - In the Alerts view you can see a list of alerts collected from various sources. You can browse through various alerts, filter them, and group them to create incidents.
3. **Remediation** - In the Remediation view, you can see a list of all remediation tasks created for various incidents. You can manage and track the remediation tasks, and push them to helpdesk if required and track the incident to closure.
4. **Configure** - In the Configuration view you can configure notification settings, third party system integration for incident management, set up aggregation rules to automate the incident management workflow for automatically creating incidents.

Review Alerts

The following tasks are performed as part of reviewing alerts:

- Understand the Alerts View.
- Filter Alerts as required, based on source type, severity, and so on.
- Create an Incident Manually.
- Add Alerts to an Existing Incident.
- Delete Alerts as required.

Filter Alerts

This procedure is useful when you want to look at alerts with a particular criteria, for example, alerts from a particular source, alerts of a particular severity, alerts from a source that are not part of an incident, and so on. Additionally, you can drill down to specifics of an alert to analyze it and investigate further into an alert if required.

Prerequisites

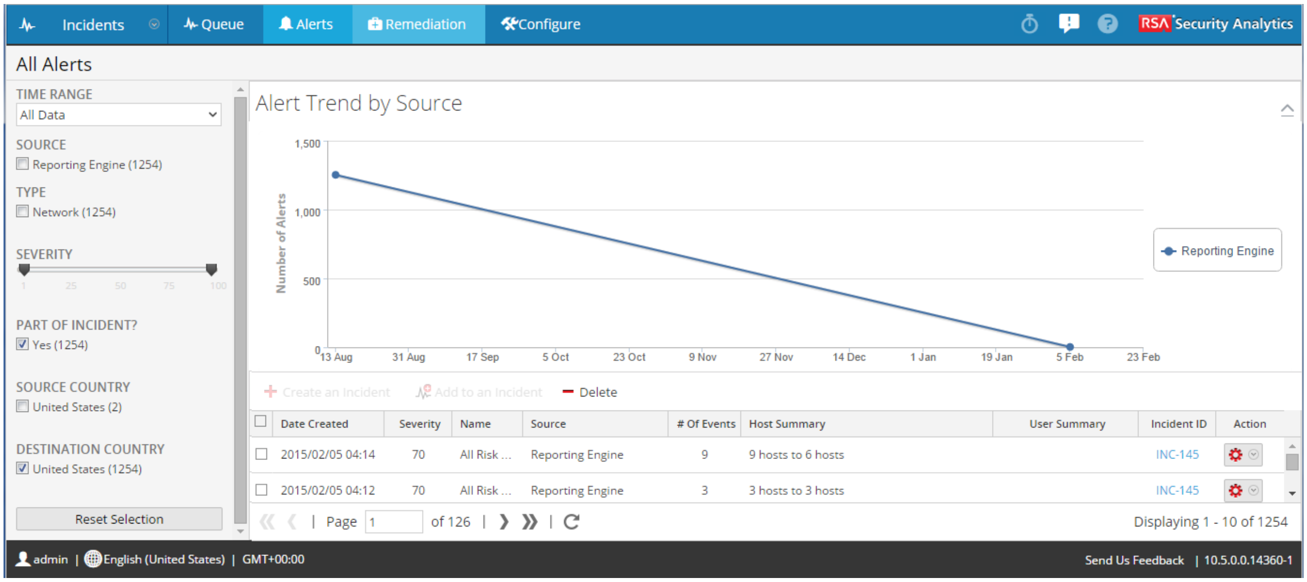
Ensure that you understand the Alert view parameters before you proceed to filter the Alerts view. For more information, see Alerts View.

Procedure

The following example describes how you can customize the view to display all ESA alerts with severity level 5.

1. In the **Security Analytics** menu, select **Incidents** > **Alerts**.

   The **All Alerts** view is displayed.



TIME RANGE
All Data

SOURCE
☐ Reporting Engine (1254)

TYPE
☐ Network (1254)

SEVERITY

PART OF INCIDENT?
☑ Yes (1254)

SOURCE COUNTRY
☐ United States (2)

DESTINATION COUNTRY
☑ United States (1254)

☐	Date Created	Severity	Name	Source	# Of Events	Host Summary	User Summary	Incident ID	Action
☐	2015/02/05 04:14	70	All Risk ...	Reporting Engine	9	9 hosts to 6 hosts		INC-145	
☐	2015/02/05 04:12	70	All Risk ...	Reporting Engine	3	3 hosts to 3 hosts		INC-145	

Page 1 of 126

Displaying 1 - 10 of 1254

admin | English (United States) | GMT+00:00

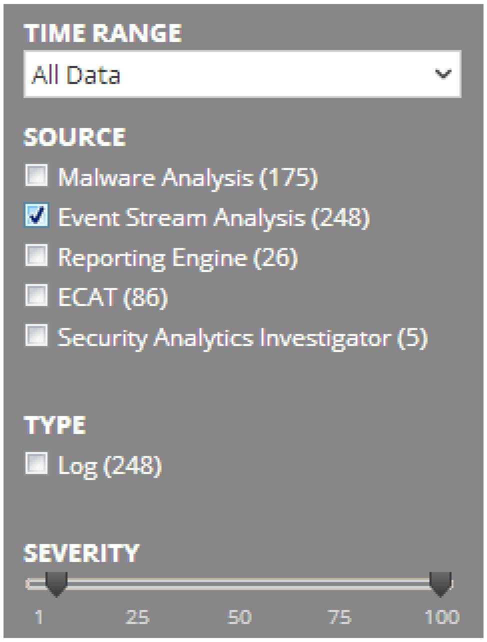
| 10.5.0.0.14360-1

2. In the options panel, select **All Data** for **TIME RANGE**.

> **Note:** By default, alerts from the last 5 days are displayed. To see alerts for a different period, change the time range.

3. Select **Event Stream Analysis** as **SOURCE**.

4. Set the **SEVERITY** level to **5**.



TIME RANGE

All Data

SOURCE

□ Malware Analysis (175)

☑ Event Stream Analysis (248)

□ Reporting Engine (26)

□ ECAT (86)

□ Security Analytics Investigator (5)

TYPE

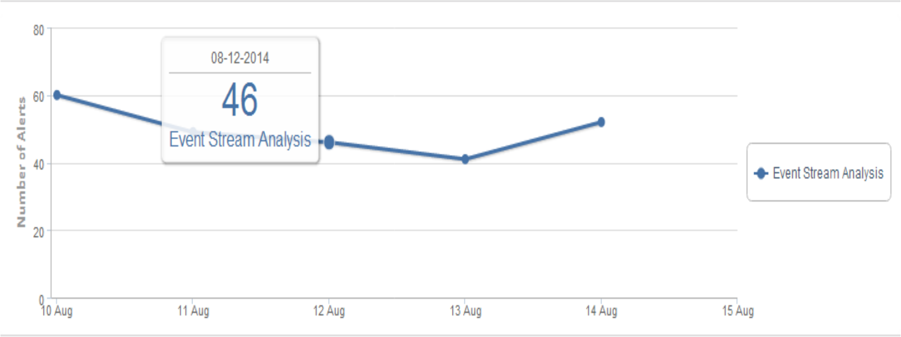
□ Log (248)

SEVERITY

The right side panel shows a graphical representation of all ESA alerts of sev 5.

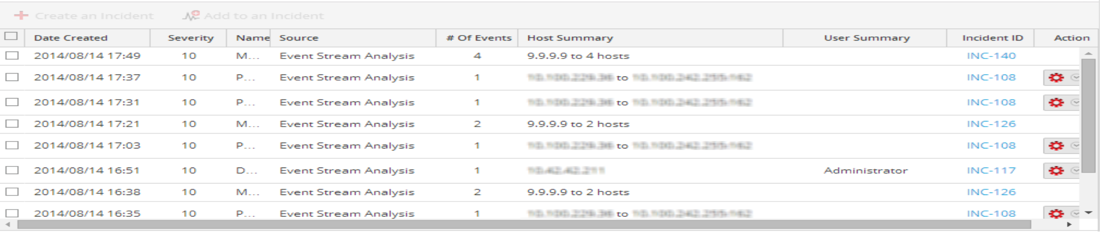
> **Note:** When there is no data for a selected filter, the filter will be disabled. Click **Reset Selection** to display default selection criteria. This applies to alerts, incidents, and remediations. For example, in the previous graphic if you change Time Range to Last Hour and there are no alerts for ESA in the last hour, source Event Stream Analysis (0) will be grayed out. In such a case, click Reset Selection. Default criteria for all options is displayed.

5. Hover on the graph to view details about the number of alerts triggered on a particular day.



The alert details are displayed in the details view in the bottom half of the page.

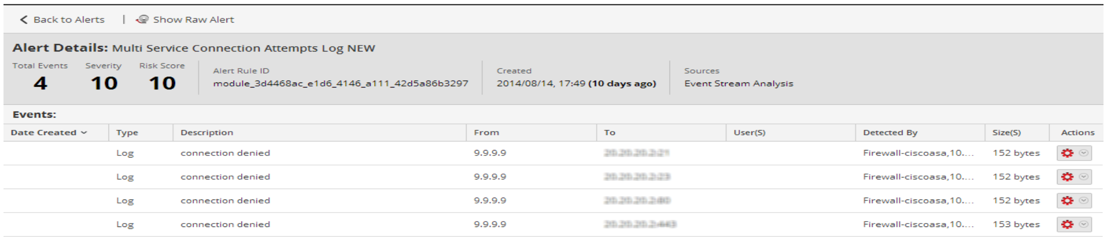
> **Note:** You can select an alert to create incidents, add an alert to an existing incident, or investigate an alert from this view. For more details see Add Alerts to an Existing Incident.



☐	Date Created	Severity	Name	Source	# Of Events	Host Summary	User Summary	Incident ID	Action
☐	2014/08/14 17:49	10	M...	Event Stream Analysis	4	9.9.9.9 to 4 hosts		INC-140	
☐	2014/08/14 17:37	10	P...	Event Stream Analysis	1	[redacted] to [redacted]		INC-108	⚙
☐	2014/08/14 17:31	10	P...	Event Stream Analysis	1	[redacted] to [redacted]		INC-108	⚙
☐	2014/08/14 17:21	10	M...	Event Stream Analysis	2	9.9.9.9 to 2 hosts		INC-126	
☐	2014/08/14 17:03	10	P...	Event Stream Analysis	1	[redacted] to [redacted]		INC-108	⚙
☐	2014/08/14 16:51	10	D...	Event Stream Analysis	1	[redacted]	Administrator	INC-117	⚙
☐	2014/08/14 16:38	10	M...	Event Stream Analysis	2	9.9.9.9 to 2 hosts		INC-126	
☐	2014/08/14 16:35	10	P...	Event Stream Analysis	1	[redacted] to [redacted]		INC-108	⚙

6. Double-click on an alert.

   The Alert Details view is displayed.



Alert Details: Multi Service Connection Attempts Log NEW

Total Events 4 | Severity 10 | Risk Score 10 | Alert Rule ID module_3d4468ac_e1d6_4146_a111_42d5a86b3297 | Created 2014/08/14, 17:49 **(10 days ago)** | Sources Event Stream Analysis

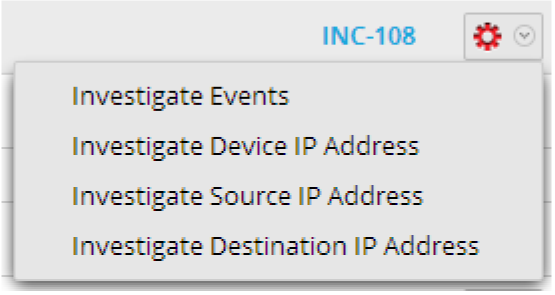
Events:

Date Created	Type	Description	From	To	User(S)	Detected By	Size(S)	Actions
	Log	connection denied	9.9.9.9	[redacted]		Firewall-ciscoasa,10....	152 bytes	⚙
	Log	connection denied	9.9.9.9	[redacted]		Firewall-ciscoasa,10....	152 bytes	⚙
	Log	connection denied	9.9.9.9	[redacted]		Firewall-ciscoasa,10....	152 bytes	⚙
	Log	connection denied	9.9.9.9	[redacted]		Firewall-ciscoasa,10....	153 bytes	⚙

The date of creation, the type of alert, description of the alert, the number of events, the user and file information, and the size of the alert are the details displayed. You can investigate the alert further as required.

Note: You can click Show Raw Alert to view the alert information in the raw format.

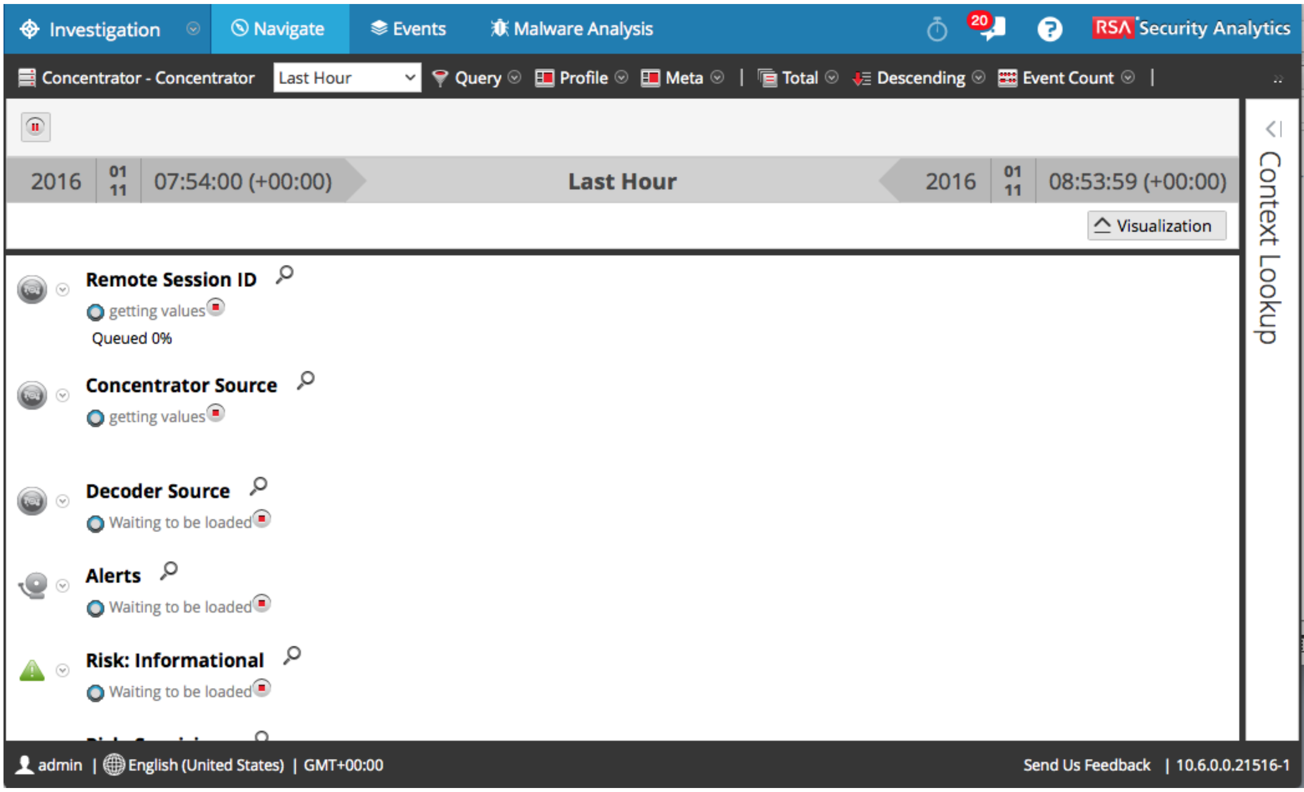
7. Under the **Actions** column, select **Investigate Events**.



INC-108
Investigate Events
Investigate Device IP Address
Investigate Source IP Address
Investigate Destination IP Address

Note: The available options under the actions menu is different for different types of Alerts. For details, see Alerts View.

The **Investigate > Navigate** view of the service is displayed. You can select the options available to investigate further.



8. Click **Back to Alerts** to navigate to the **All Alerts** view.

9. If you want to restore defaults, click **Reset Selection**.

For details on various parameters and description in the **Incidents** > **All Alerts** view, see Alerts View.

Create an Incident Manually

This procedure is helpful when an analyst wants to browse through various alerts, select the required alerts to group them, and create an incident to include the selected alerts.

Note: Incidents can be created manually or automatically. An Alert can only be associated with one Incident. For automatic creation of incidents you have to create aggregation rules that would analyze the alerts collected and group them into incidents automatically depending on which rules they match. For details, see Create an Aggregation Rule.

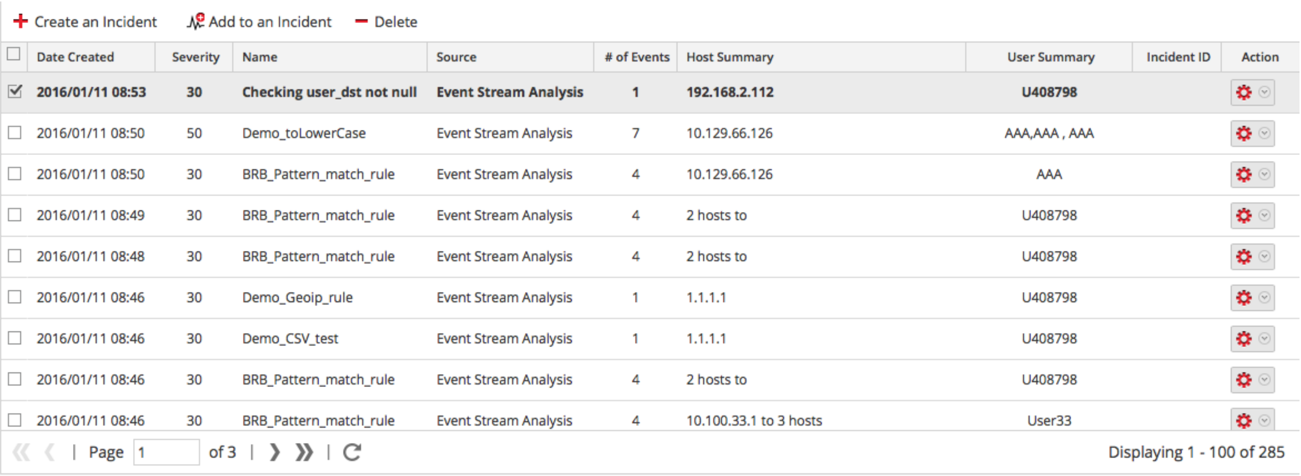
To create an incident manually:

1. In the **Security Analytics** menu, select **Incidents** > **Alerts**.

   The **All Alerts** view is displayed.

2. Select one or more alerts in the alert details view in the right hand bottom half of the page

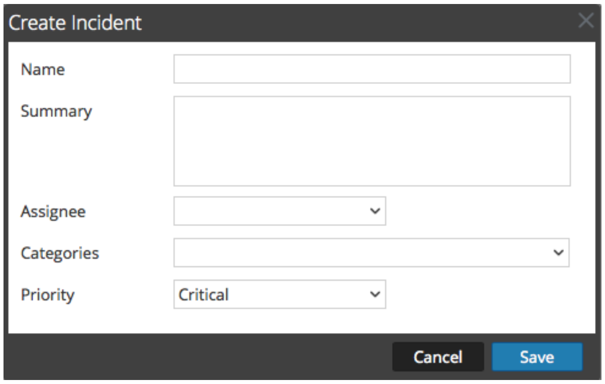
   Note: Only when you select alerts that have no Incident ID mentioned, the **Create an Incident** option is enabled, else it is disabled if the alert is already part of an incident. You can filter alerts that are not part of any incident by selecting the option **Part of an Incident** as **No** in the options panel.



☐	Date Created	Severity	Name	Source	# of Events	Host Summary	User Summary	Incident ID	Action
☑	**2016/01/11 08:53**	**30**	**Checking user_dst not null**	**Event Stream Analysis**	**1**	**192.168.2.112**	**U408798**		⚙
☐	2016/01/11 08:50	50	Demo_toLowerCase	Event Stream Analysis	7	10.129.66.126	AAA,AAA , AAA		⚙
☐	2016/01/11 08:50	30	BRB_Pattern_match_rule	Event Stream Analysis	4	10.129.66.126	AAA		⚙
☐	2016/01/11 08:49	30	BRB_Pattern_match_rule	Event Stream Analysis	4	2 hosts to	U408798		⚙
☐	2016/01/11 08:48	30	BRB_Pattern_match_rule	Event Stream Analysis	4	2 hosts to	U408798		⚙
☐	2016/01/11 08:46	30	Demo_Geoip_rule	Event Stream Analysis	1	1.1.1.1	U408798		⚙
☐	2016/01/11 08:46	30	Demo_CSV_test	Event Stream Analysis	1	1.1.1.1	U408798		⚙
☐	2016/01/11 08:46	30	BRB_Pattern_match_rule	Event Stream Analysis	4	2 hosts to	U408798		⚙
☐	2016/01/11 08:46	30	BRB_Pattern_match_rule	Event Stream Analysis	4	10.100.33.1 to 3 hosts	User33		⚙

3. Click **Create an Incident**.

   The **Create Incident** dialog is displayed.



4. Provide the following information:

   Name - Type a name to identify the incident.

   Summary - (Optional) Type a description for the incident.

   Assignee - (Optional) Select a assignee to whom the incident is assigned.

   Categories - (Optional) Select one or more categories to which the incident belongs.

   Priority - Select a priority for the incident from the options Critical, High, Medium, or Low displayed in the drop-down list.

5. Click **Save**.

   The incident is saved and displayed in the **Incidents** > **Queue** > **All Incidents** view.

   > **Note:** If you assign the incident to yourself, the incident will be saved and displayed in the **Incidents** > **Queue** > **My Incidents** view.

Add Alerts to an Existing Incident

This procedure is required when you have an alert with a particular criteria that fits an existing incident and you do not have to create a new incident.

To add an alert to an existing incident:

1. In the **Security Analytics** menu, select **Incidents > Alerts**.

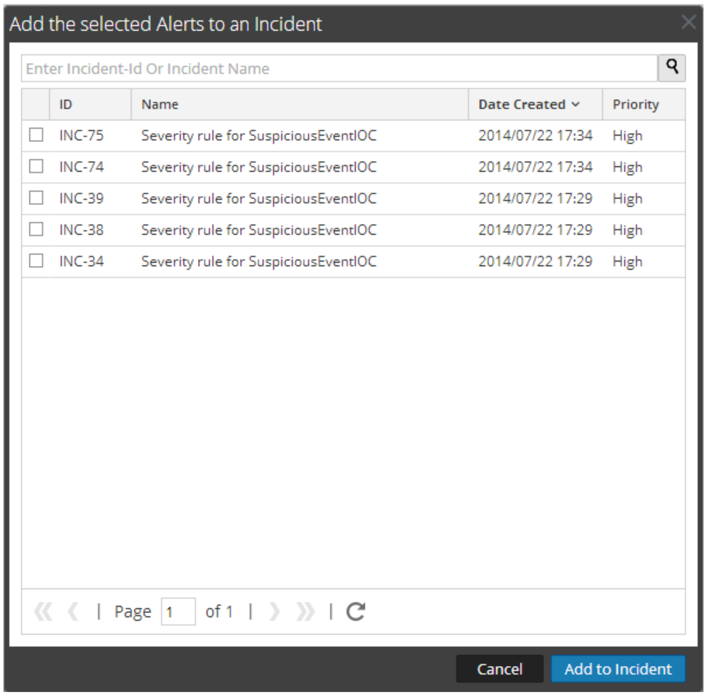
   The **All Alerts** view is displayed.

2. In the alert details view in the right-hand bottom half of the page, select one or more alerts that need to be added to an incident.

3. Click Add to an Incident .

   The **Add the selected Alerts to an Incident** dialog is displayed.

   All the incidents assigned to you that are still open are displayed. You can search within the dialog to narrow down the list.



Add the selected Alerts to an Incident

Enter Incident-Id Or Incident Name

	ID	Name	Date Created	Priority
□	INC-75	Severity rule for SuspiciousEventIOC	2014/07/22 17:34	High
□	INC-74	Severity rule for SuspiciousEventIOC	2014/07/22 17:34	High
□	INC-39	Severity rule for SuspiciousEventIOC	2014/07/22 17:29	High
□	INC-38	Severity rule for SuspiciousEventIOC	2014/07/22 17:29	High
□	INC-34	Severity rule for SuspiciousEventIOC	2014/07/22 17:29	High

Note: Only when you have an alert that does not have an incident ID assigned, the **Add to an Incident** option is enabled, else it is disabled if the alert is already part of an incident.

4. Select an incident from the list displayed to which the alert needs to be added.

5. Click **Add to Incident**.

   The selected alert or alerts are now part of the incident chosen and will have an incident ID.

Delete Alerts

This procedure is helpful when there are unwanted or non-relevant alerts. Deleting these alerts frees up disk space.

Prerequisites

The Administrator role must be assigned to you.

Procedure

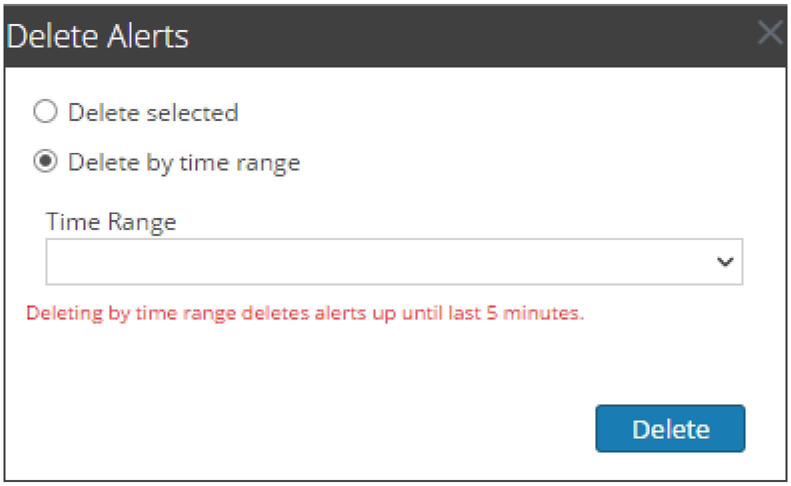
To delete alerts:

1. In the **Security Analytics** menu, select **Incidents** > **Alerts**.

   The All Alerts view is displayed.

2. If you want to delete certain alerts, select each alert.

3. Click − Delete .

   Delete Alerts

   ○ Delete selected

   ● Delete by time range

   Time Range

   Deleting by time range deletes alerts up until last 5 minutes.

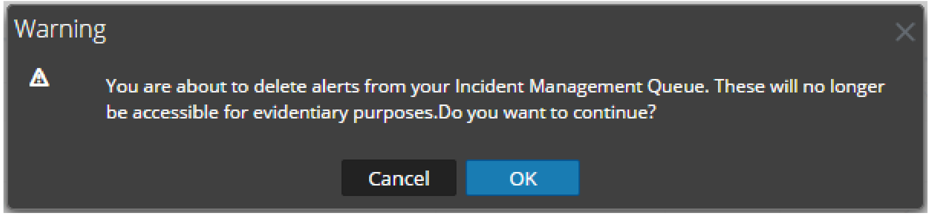
4. Perform one of the following actions:

   - Click **Delete selected** to delete previously selected alerts.
   - Select **Delete by time range** and choose the time range, then click **Delete**.

Note: When you delete by time range, you delete alerts up until the last hour.

5. Click **OK**.

   A confirmation dialog is displayed.



Warning

⚠ You are about to delete alerts from your Incident Management Queue. These will no longer be accessible for evidentiary purposes.Do you want to continue?

6. Click **OK** to delete the alerts.

Result

Each selected alert is deleted. The following conditions apply:

- If a deleted alert is the only alert in an incident, the incident is also deleted.
- If the deleted alert is not the only alert in an incident, the incident is updated to reflect the deletion.
- You can manually add an alert that was part of a deleted incident to a new or existing incident.
- The rule engine will not automatically pick up any alert that was part of a deleted incident.

Incident Management Process Flow

As part of the Incident Management process flow, you can edit incidents to modify their parameters as required, delete incidents, assign the incidents to different users, and track and monitor them to closure.

The following list introduces various tasks that are performed as part of the Incident Management process:

- View Incident Queue
- View Incident Details
- Edit Incidents
- Investigate an Incident
  - Add a Journal Entry
  - Create a Remediation Task
  - Send a Remediation Task as a Helpdesk Ticket
  - Send a Remediation Task to RSA Archer
  - Close an Incident
- Delete Incidents

View Incident Queue

Administrators and analysts can view incidents in the Incidents Queue. You can see your assigned incidents or all incidents, and view the queue using different filters.

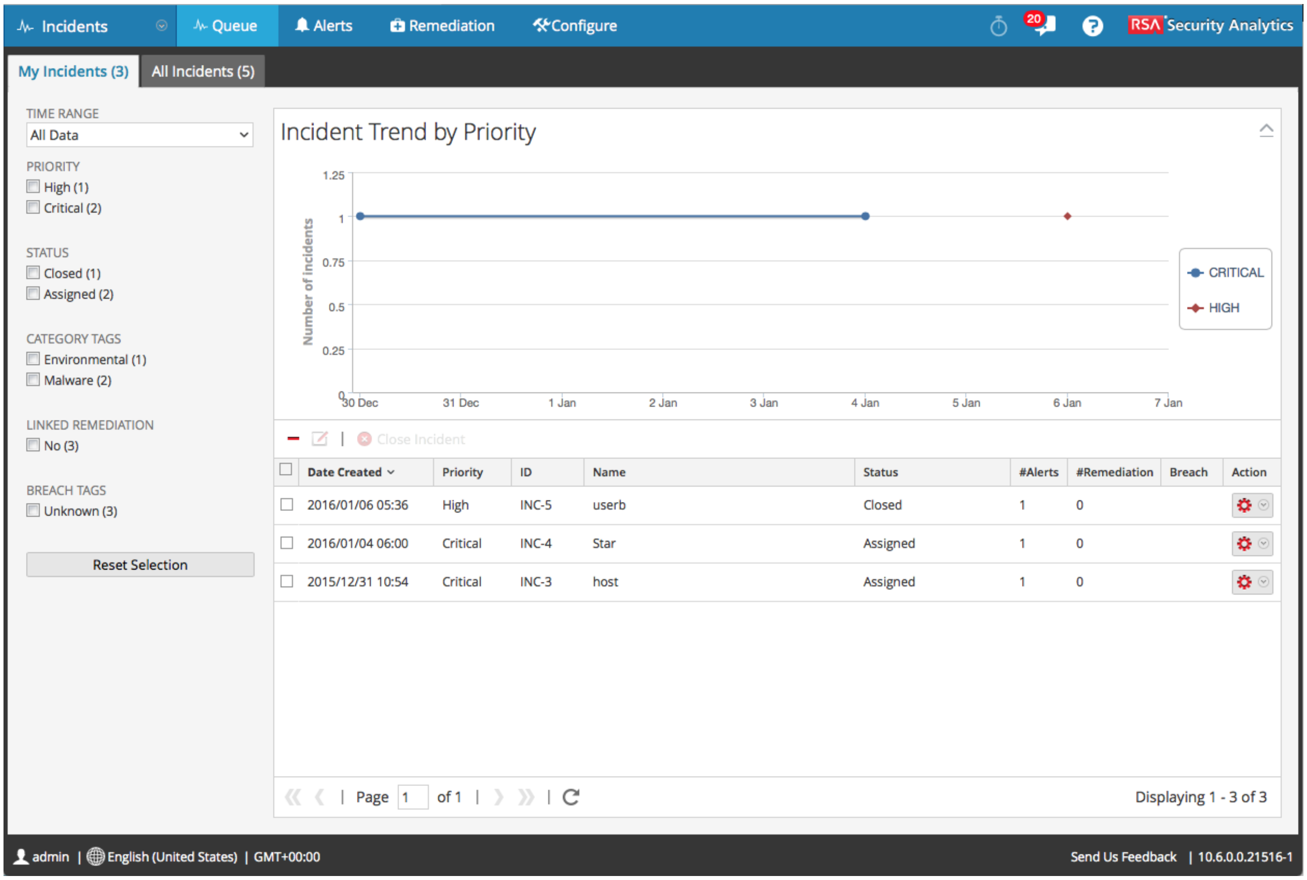
To view the Incident queue:

1. In the **Security Analytics** menu, select **Incidents** > **Queue**.

   The **My Incidents** view is displayed by default. This displays a list of incidents assigned to you.

   The right hand panel displays the graphical representation of the incidents assigned to you. The graph displays the incident trend by priority and is one line per priority.

   For details on various parameters displayed and their description, see Incident Queue View.



TIME RANGE
All Data

PRIORITY
□ High (1)
□ Critical (2)

STATUS
□ Closed (1)
□ Assigned (2)

CATEGORY TAGS
□ Environmental (1)
□ Malware (2)

LINKED REMEDIATION
□ No (3)

BREACH TAGS
□ Unknown (3)

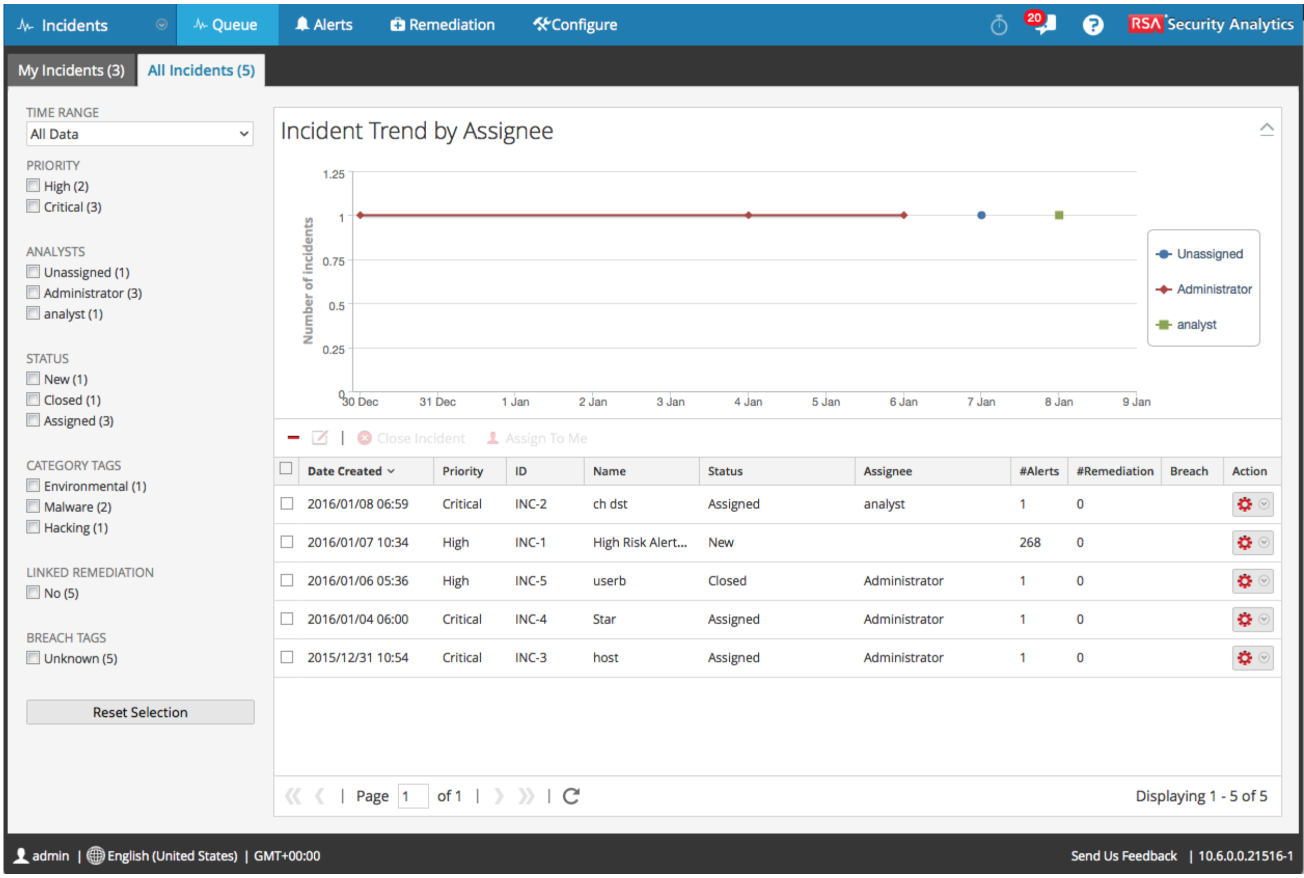
□	Date Created	Priority	ID	Name	Status	#Alerts	#Remediation	Breach	Action
□	2016/01/06 05:36	High	INC-5	userb	Closed	1	0		
□	2016/01/04 06:00	Critical	INC-4	Star	Assigned	1	0		
□	2015/12/31 10:54	Critical	INC-3	host	Assigned	1	0		

2. Select **All Incidents**.

   The All Incidents view is displayed with a list of all incidents.

   The right hand panel displays the graphical representation of the incident trend by assignee and is one line per assignee.

For details on various parameters displayed and their description, see Incident Queue View.



TIME RANGE
All Data

PRIORITY
□ High (2)
□ Critical (3)

ANALYSTS
□ Unassigned (1)
□ Administrator (3)
□ analyst (1)

STATUS
□ New (1)
□ Closed (1)
□ Assigned (3)

CATEGORY TAGS
□ Environmental (1)
□ Malware (2)
□ Hacking (1)

LINKED REMEDIATION
□ No (5)

BREACH TAGS
□ Unknown (5)

□	Date Created	Priority	ID	Name	Status	Assignee	#Alerts	#Remediation	Breach	Action
□	2016/01/08 06:59	Critical	INC-2	ch dst	Assigned	analyst	1	0		
□	2016/01/07 10:34	High	INC-1	High Risk Alert...	New		268	0		
□	2016/01/06 05:36	High	INC-5	userb	Closed	Administrator	1	0		
□	2016/01/04 06:00	Critical	INC-4	Star	Assigned	Administrator	1	0		
□	2015/12/31 10:54	Critical	INC-3	host	Assigned	Administrator	1	0		

| Page 1 of 1 | Displaying 1 - 5 of 5

View Incident Details

This procedure is required when you need to further investigate an incident and decide on how to proceed with remediation of the incident and track it to closure.

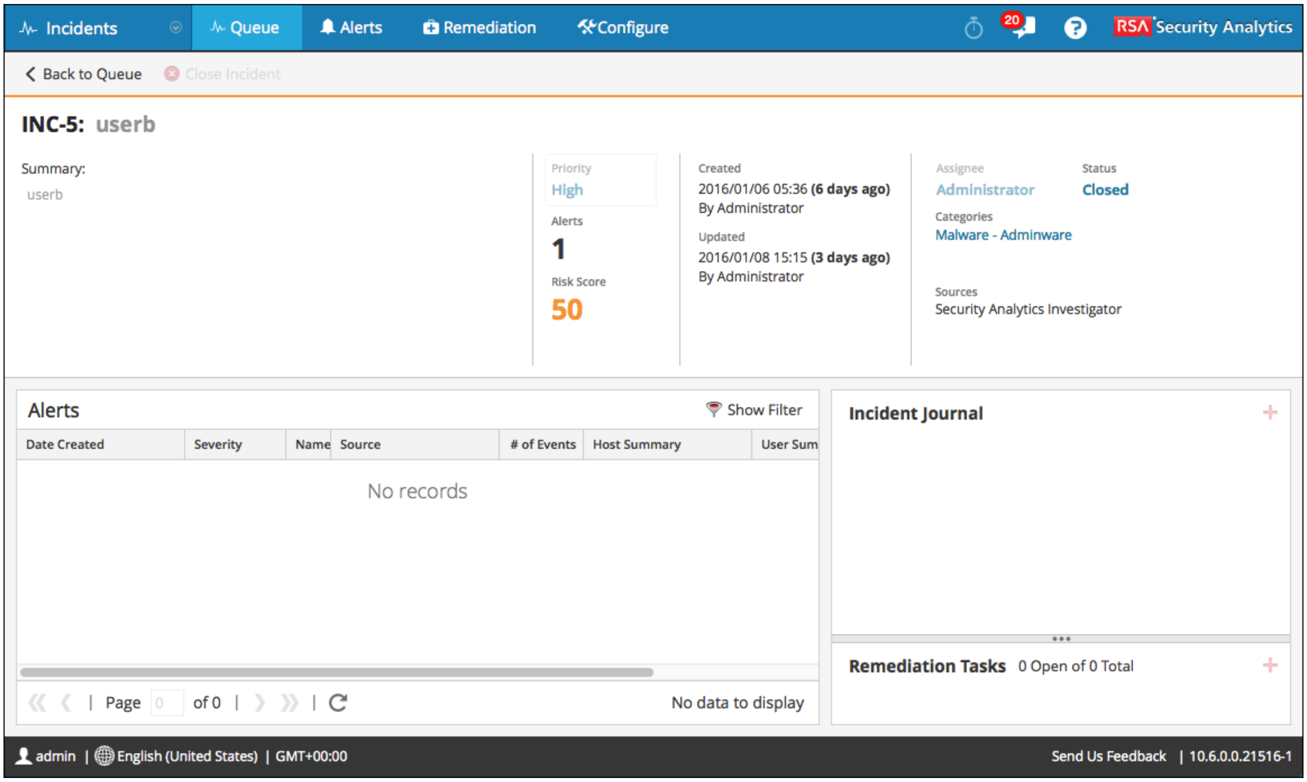
To access and view incident details:

1. In the **Security Analytics** menu, select **Incidents** > **Queue**.

   The **My Incidents** view is displayed. It lists all the incidents that are assigned to you. The **All Incidents** view lists all the incidents in Security Analytics.

2. In the **My Incidents** view, double-click an incident.

   The Incident details page is displayed.



INC-5: userb

Summary: userb

Priority: High

Alerts: 1

Risk Score: 50

Created: 2016/01/06 05:36 (**6 days ago**) By Administrator

Updated: 2016/01/08 15:15 (**3 days ago**) By Administrator

Assignee: Administrator

Status: Closed

Categories: Malware - Adminware

Sources: Security Analytics Investigator

Alerts

Date Created	Severity	Name	Source	# of Events	Host Summary	User Sum

No records

No data to display

Incident Journal

Remediation Tasks 0 Open of 0 Total

admin | English (United States) | GMT+00:00

Send Us Feedback | 10.6.0.0.21516-1

The Incident details page displays all the details pertaining to the incident. You can analyze the data and perform the following operations from this view:

- Discover the context and risk of the Incident by viewing the Alerts and/or their Events, or using the action menu to investigate related events.
- Track the progress of the workflow on the Incident by assigning it to the right analyst, setting the priority, recording the status of the investigation, or categorizing the Incident.

- Document the investigation results using the Incident Journal, or track the remediation process using Remediation Tasks.
- In cases where there is evidence of a data breach, report it to the compliance team.
- Close the Incident once the investigation is completed.

3. Click **Back to Queue** to return to the Incidents view.

Edit Incidents

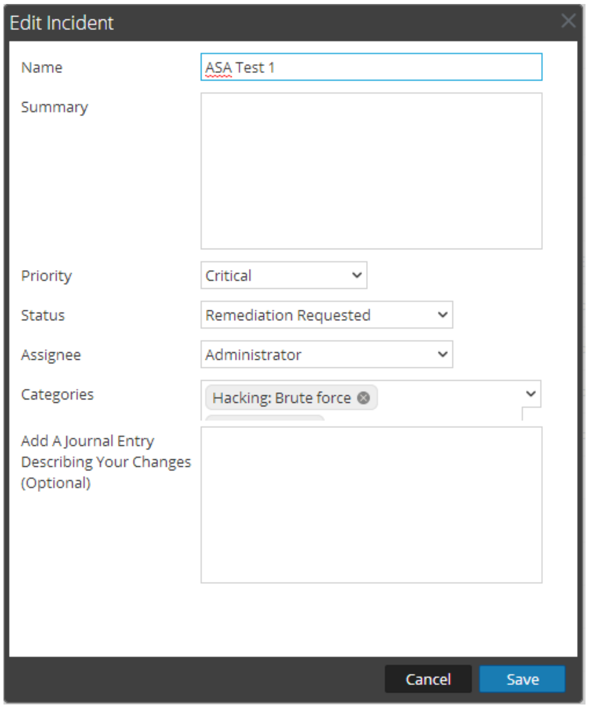
You can edit incidents in one of the following ways:

- **Edit an incident** - Use this when you need to modify particulars of a single incident.
- **Edit incidents in bulk** - Use this when you have to modify a particular criteria for multiple incidents.

Edit an Incident

1. In the **Security Analytics** menu, select **Incidents** > **Queue**.
2. In the **All Incidents** view, select an incident.
3. Click 📝.

   The **Edit Incident** dialog is displayed.



Edit Incident

Name	ASA Test 1
Summary	
Priority	Critical
Status	Remediation Requested
Assignee	Administrator
Categories	Hacking: Brute force
Add A Journal Entry Describing Your Changes (Optional)	

Note: Alternatively you can select Edit Incident under the actions column for the selected incident.

4. Modify the required values.
5. Click **Save**.

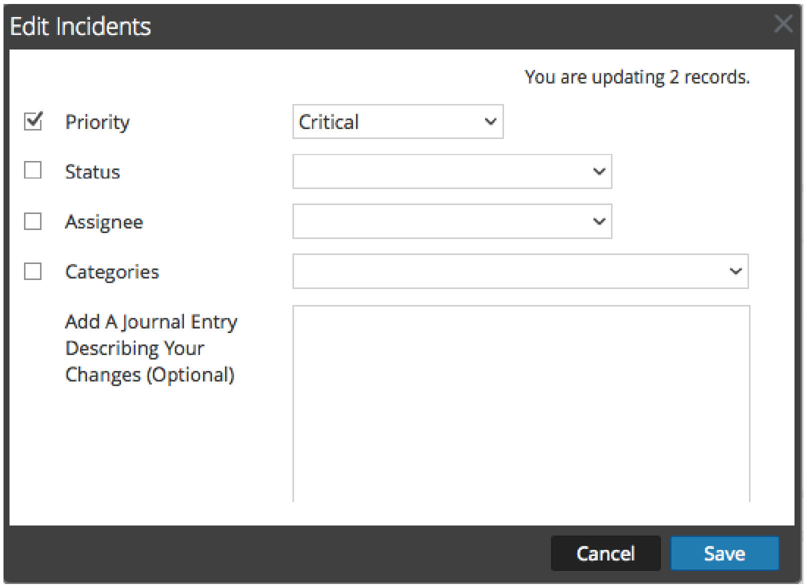
   The edited incident is displayed in the **All Incidents** view.

Note: This procedure can be performed in a similar way in the My Incident view as well.

Edit Incidents in Bulk

1. In the **Security Analytics** menu, select **Incidents** > **Queue**.
2. In the **All Incidents** view, select 2 or more incidents.
3. Click 📝.

   The **Edit Incidents** dialog is displayed.



Edit Incidents

You are updating 2 records.

☑ Priority: Critical

□ Status

□ Assignee

□ Categories

Add A Journal Entry Describing Your Changes (Optional)

4. Modify the required values.

   The values that can be modified in bulk are Priority, Status, Assignee, and Categories. If you select a checkbox, any modifications in the values for that field (including clearing the value) are applied for that field for all selected Incidents. If the checkbox is not selected, that field is unchanged for the selected Incidents.
5. Click **Save**.

   The edited incidents are displayed in the **All Incidents** view.

Note: This procedure can be performed in a similar way in the **My Incidents** view as well.

Investigate an Incident

Once you create an incident manually or by using an automated process, the next step is to further investigate the incident, create a remediation task, add journal entries to include specifics and additional information for the incident, track the remediation tasks to closure, push the tasks as help desk tickets to resolve them, and finally decommission the incident.

The various stages of investigating an incident and the actions performed by an administrator are outlined in the table below.

Tasks	Reference
1. Access and view incident details.	Refer to View Incident Details.
2. Add a journal entry.	Refer to Add a Journal Entry.
3. Create and track a remediation task.	Refer to Create a Remediation Task.
4. Push a remediation task as a Help Desk ticket	Refer to Send a Remediation Task as a Helpdesk Ticket.
5. Close an incident.	Refer to Close an Incident.

Topics

- Add a Journal Entry
- Create a Remediation Task
- Send a Remediation Task as a Helpdesk Ticket
- Send a Remediation Task to RSA Archer
- Close an Incident

Add a Journal Entry

You create a journal entry for an incident to capture additional information regarding the incident that helps the assignee understand the incident and track it in a better way.

Procedure

To create a journal entry for an incident:

1. In the **Security Analytics** menu, select **Incidents** > **Queue**.

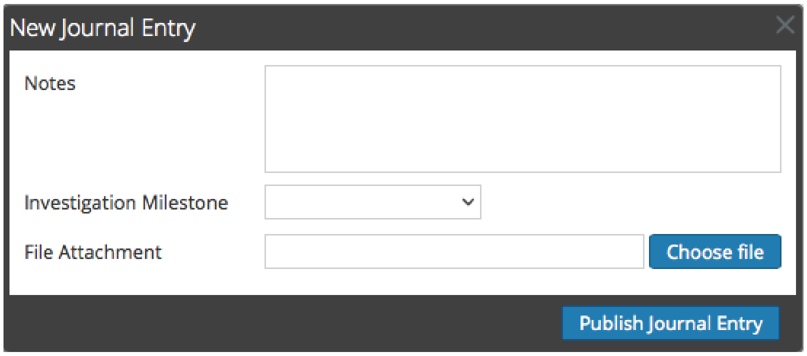
   The My Incidents view is displayed.

2. In the **My Incidents** view, double-click an incident.

   The incident details view is displayed.

3. Under **Incident Journal**, click +

   The New Journal Entry dialog is displayed.

4. Provide the required information. The Notes field is required. Type in relevant useful information in the Notes field to describe the investigation. The Investigation Milestone and file attachments are optional and can be included when it is useful for further investigation. The Investigation Milestone options are: Reconnaissance, Delivery, Exploitation, Installation, Command and Control, Action On Objective, Containment, Eradication, and Closure.

5. Click **Publish Journal Entry**.

   The journal entry is created and displayed under **Incident Journal**.

Create a Remediation Task

When you have investigated an incident and have identified the cause, you can create a remediation task, assign it to a particular group and track it to closure.

Procedures

Create a Remediation Task

1. In the Security Analytics menu, select **Incidents** > **Queue**.

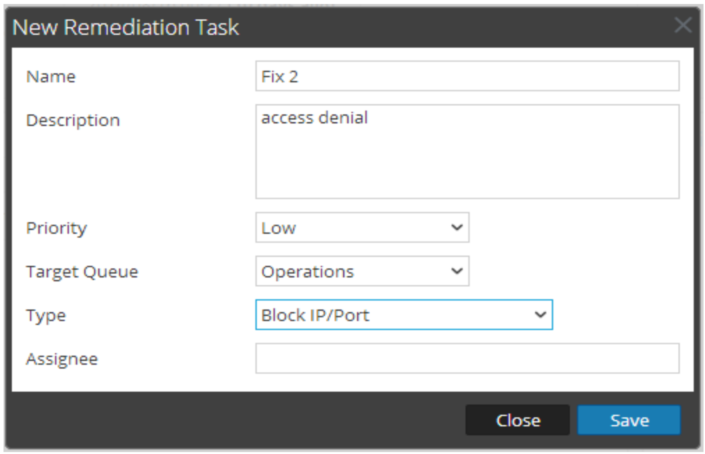
   The My Incidents tab is displayed.

2. In the **My Incidents** tab, double-click an incident.

   The incident details view is displayed.

3. Under **Remediation Tasks**, click +

   The New Remediation Task dialog is displayed.



New Remediation Task

Name: Fix 2

Description: access denial

Priority: Low

Target Queue: Operations

Type: Block IP/Port

Assignee:

4. Provide the following information:

   Name - Name of the remediation task.

   Description - (Optional) Type information that describes the remediation task.

   Priority - Select the priority for the task: Low, Medium, High, or Critical.

   Target Queue - Select the target queue depending on the type of the task: Operations, GRC, or Content Improvement.

   Type - Select a type for the task: Quarantine host, Quarantine Network Device, Block IP/Port, Block External Access to DMZ, Block VPN Access, Reimage host, Update Firewall Policy, Update IDS/IPS Policy, Update Web Proxy Policy, Update Access Policy, Update VPN Policy, or Custom.

   Assignee - (Optional) Type the username of the user to whom the task is to be assigned.

5. Click **Save**.

   The remediation task is listed under Remediation tasks.

Modify a Remediation Task

1. In the Security Analytics menu, select **Incidents** > **Queue**.

   The My Incidents view is displayed.

2. In the **My Incidents** view, double-click an incident.

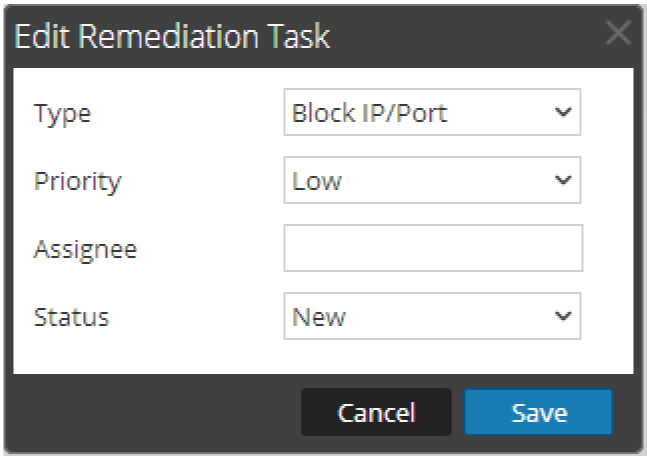
   The incident details view is displayed.

3. Under **Remediation Tasks**, double-click a remediation task.

   The remediation task details view is displayed.

4. Click Edit All.

   The Edit Remediation Task dialog is displayed.



Edit Remediation Task

Type: Block IP/Port

Priority: Low

Assignee:

Status: New

5. Modify the required fields.

6. Click **Save**.

Note: Alternatively, you can click the parameter that you want to modify in the top panel and modify the value as required.

Send a Remediation Task as a Helpdesk Ticket

You can push a remediation task as a Helpdesk ticket where it can be managed in a third party helpdesk system and tracked to closure.

Prerequisites

Ensure you have enabled the integration with the third party helpdesk ticketing system. See Configure Integration Setting to Manage Incidents in Security Analytics for details.

Procedure

To push a remediation task as a helpdesk ticket:

1. In the **Security Analytics** menu, select **Incidents** > **Queue**.

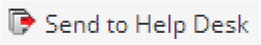
   The My Incidents view is displayed.

2. In the **My Incidents** view, double-click an incident.

   The Incident Details view is displayed.

3. Under **Remediation Tasks**, double-click a remediation task.

   The Remediation Task Details view is displayed.

4. Click  Send to Help Desk

   The remediation task is pushed to the helpdesk ticketing system.

5. Click View Ticket in Helpdesk to view the ticket in the helpdesk system.

Send a Remediation Task to RSA Archer

You can push the remediation tasks to the Archer target queue and report data breaches and track them through the breach response process in the RSA Security Operations Management solution.

Prerequisites

Ensure you have enabled the integration with the RSA Archer. See Configure Integration Setting to Manage Incidents in RSA Archer Security Operations for details.

Procedure

To push a remediation task to RSA Archer:

1. In the **Security Analytics** menu, select **Incidents** > **Queue**.

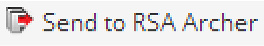
   The My Incidents view is displayed.

2. In the **My Incidents** view, double-click an incident.

   The Incident Details view is displayed.

3. Under **Remediation Tasks** double-click a remediation task.

   The Remediation Task Details view is displayed.

4. Click .

   The remediation task is sent to RSA Archer.

5. Navigate to the RSA Archer UI to view and track the remediation task to closure.

Close an Incident

When you have arrived at a solution after investigating an incident and remediated it, you close the incident.

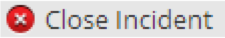
Procedure

To close an incident:

1. In the **Security Analytics** menu, select **Incidents > Queue**.

   The My Incidents view is displayed.

2. In the **My Incidents** view, select an incident.

3. Click  ⊗ Close Incident

   The Incident is closed and the status of the incident is displayed as **Closed** in the Incidents view.

Note: Alternatively, you can close the incident by selecting **Close Incident** under the **Actions** column for the incident or by selecting **Close Incident** in the Incident Details view of an incident.

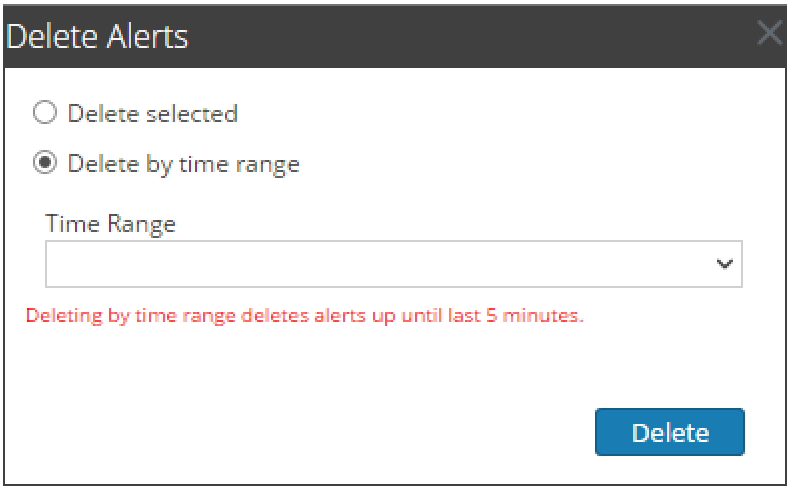
Delete Incidents

This procedure is helpful to free up disk space by deleting incidents that are not needed.

Procedure

1. In the **Security Analytics** menu, select **Incidents** > **Queue**.
   The My Incidents tab is displayed.
2. Select the **All Incidents** tab to see all incidents for all analysts.
3. Perform one of the following actions:
   - Select each incident to delete, then click − Delete .
   - Click − Delete , choose **Delete by Time Range** and select the time period to delete alerts.

3. Click **OK**.



Delete Alerts

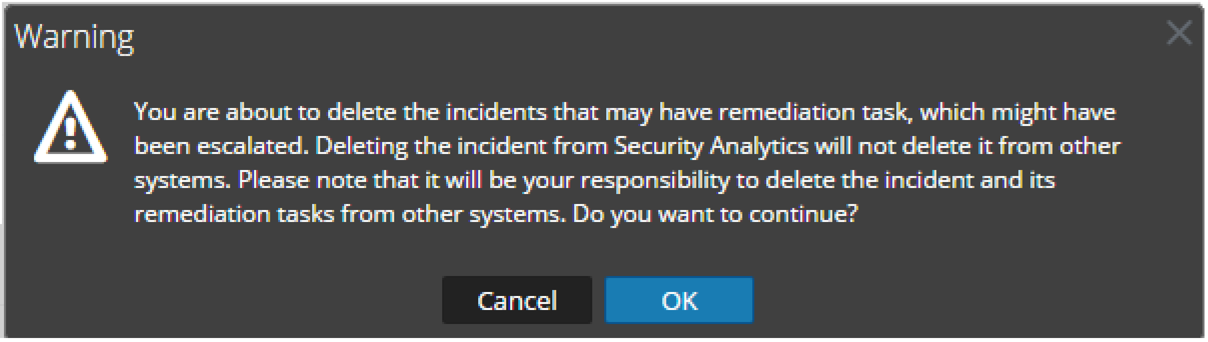
○ Delete selected

● Delete by time range

Time Range

Deleting by time range deletes alerts up until last 5 minutes.

4. A confirmation dialog is displayed.



Warning

You are about to delete the incidents that may have remediation task, which might have been escalated. Deleting the incident from Security Analytics will not delete it from other systems. Please note that it will be your responsibility to delete the incident and its remediation tasks from other systems. Do you want to continue?

5. Click **OK** to delete the incidents.

Result

Deleted incidents, which includes journal entries and remediation tasks, are deleted. The incidents are no longer accessible for evidentiary purposes.

Alerts that were associated with a deleted incident still display in the Alerts tab so you can manually add them to another incident. However, the rule engine will no longer pick up the alerts and automatically group them into incidents.

An audit log records the number of incidents that were deleted.

Automate the Incident Management Process

You can automate the workflow to avoid manual intervention wherever required for ease of use. You can create and manage users and user permissions that are required to investigate the incidents, and create aggregation rules to group alerts as per specified criteria and create incidents automatically. These incidents created are further investigated as described in Incident Management Process.

The following list shows the procedures for automating the incident management process:

- Add user with required permission to investigate incidents assigned. For more information, see **Manage Users with Roles and Permissions** in the *System Security and User Management* guide.
- Configure Notification Settings to send email notifications once the incidents are created and go through various stages of incident
- Create an Aggregation Rule to group alerts into incidents depending on the criteria set.
- Set a Retention Period for Alerts and Incidents
- Obfuscate Private Data: Hash values for meta keys that contain sensitive data such as hostnames, usernames, and IP addresses.

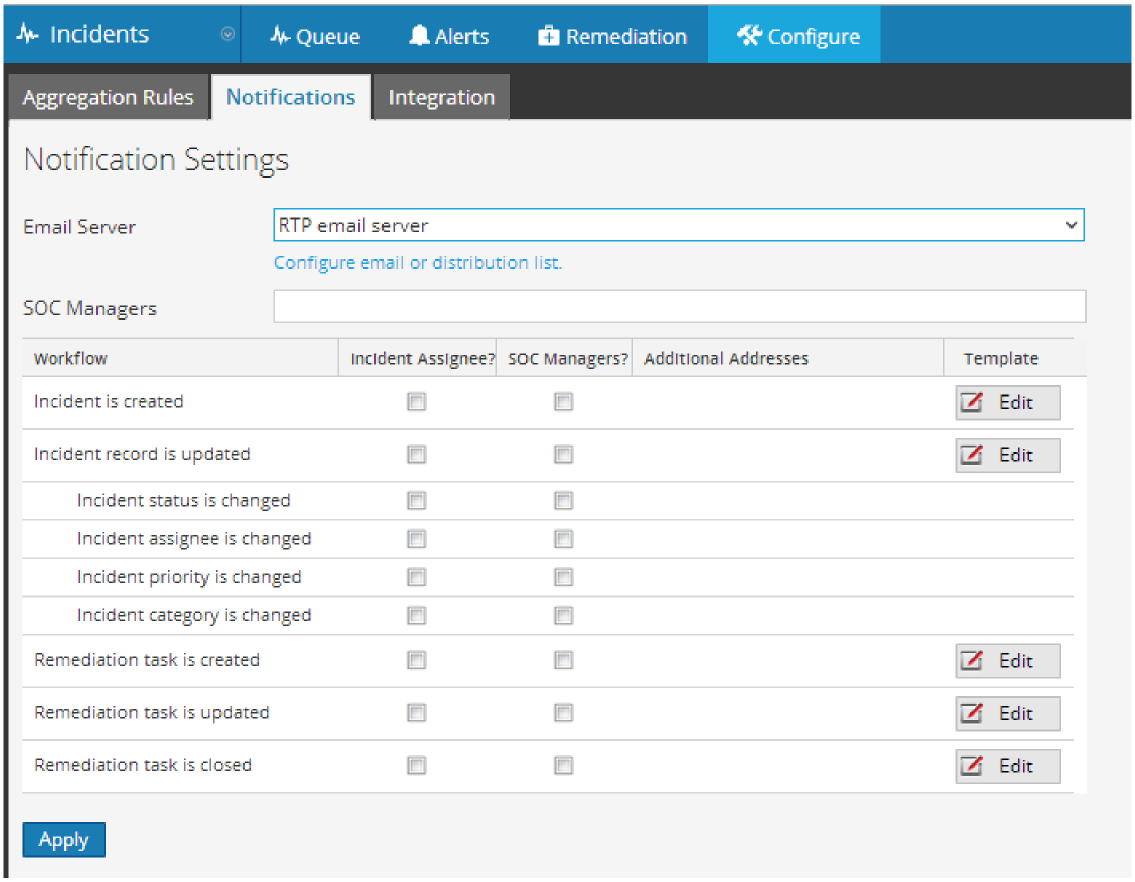
Configure Notification Settings

Configuring notification settings enables notification mechanism for various operations performed during the Incident Management workflow.

To configure notification settings:

1. In the **Security Analytics** menu, select **Incidents > Configure**.
2. Click **Notifications**.

   The Notifications Settings view is displayed.



Notification Settings

Email Server: RTP email server

SOC Managers:

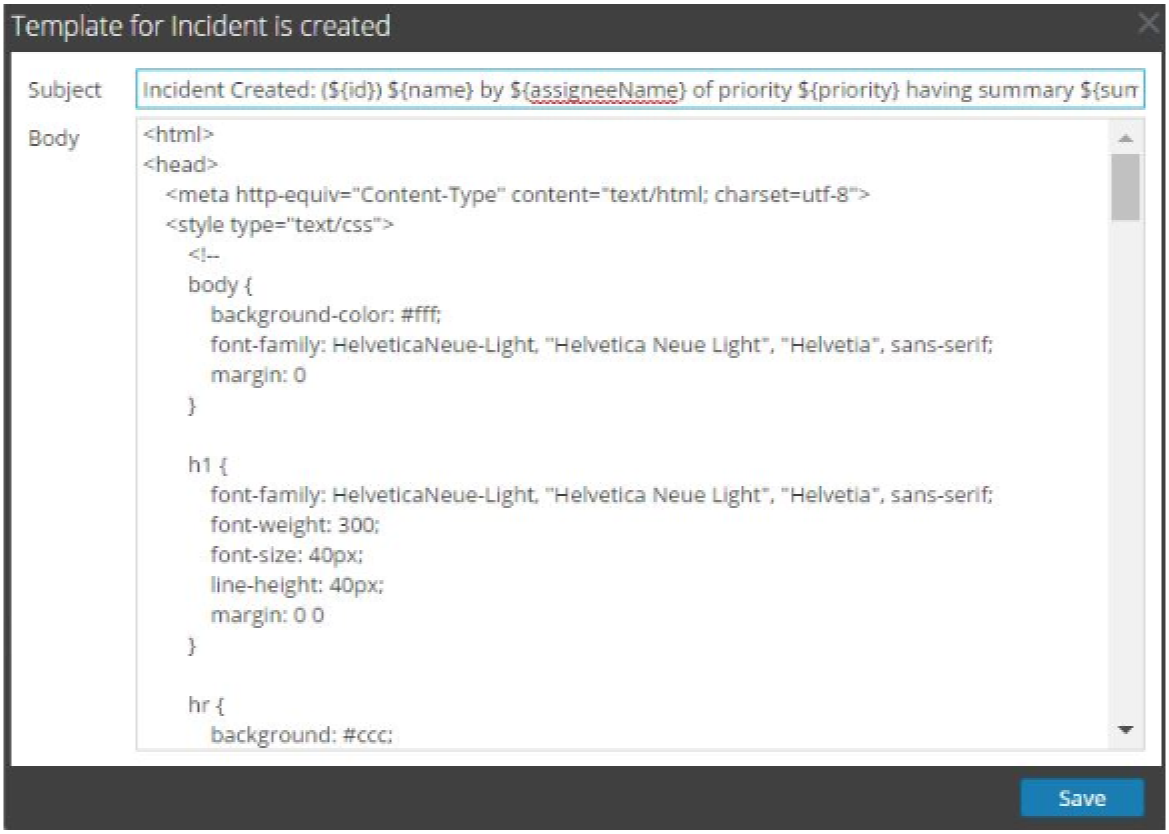
Workflow	Incident Assignee?	SOC Managers?	Additional Addresses	Template
Incident is created	□	□		Edit
Incident record is updated	□	□		Edit
Incident status is changed	□	□		
Incident assignee is changed	□	□		
Incident priority is changed	□	□		
Incident category is changed	□	□		
Remediation task is created	□	□		Edit
Remediation task is updated	□	□		Edit
Remediation task is closed	□	□		Edit

3. Provide the following information to configure various notification settings.

Parameter	Description
Email Server	Select the Email server address from the drop-down list to be configured to send out mail notification when the notification settings are enabled. If there is no email server address configured you will not see an email server listed in the drop-down list. You have to configure an email server before you can proceed with this procedure. You can configure the email server by clicking **Configure email or distribution list** and providing the required details. Refer to the **Configure Email Server and Notification Account** in the *System Configuration* guide on how to configure an email server.
SOC Managers	Type the SOC Manager email addresses to which a notification mail is sent for the selected operations.
Incident Assignee?	Select if you want a mail notification to be sent, to whom the incident is assigned, for the corresponding workflow whenever an incident is assigned.
SOC Manager?	Select if you want a mail notification to be sent to the group of SOC managers for the corresponding workflow. This corresponds to the manager email addresses provided under **SOC Managers**.
Additional Addresses	Type in additional addresses to which you want mail notifications to be sent for the corresponding workflow.

4. (Optional) In the **Template** column, click Edit to modify the template for any workflow.

   The following figure shows you an incident created template in the edit mode.



Template for Incident is created

Subject: Incident Created: (${id}) ${name} by ${assigneeName} of priority ${priority} having summary ${sum

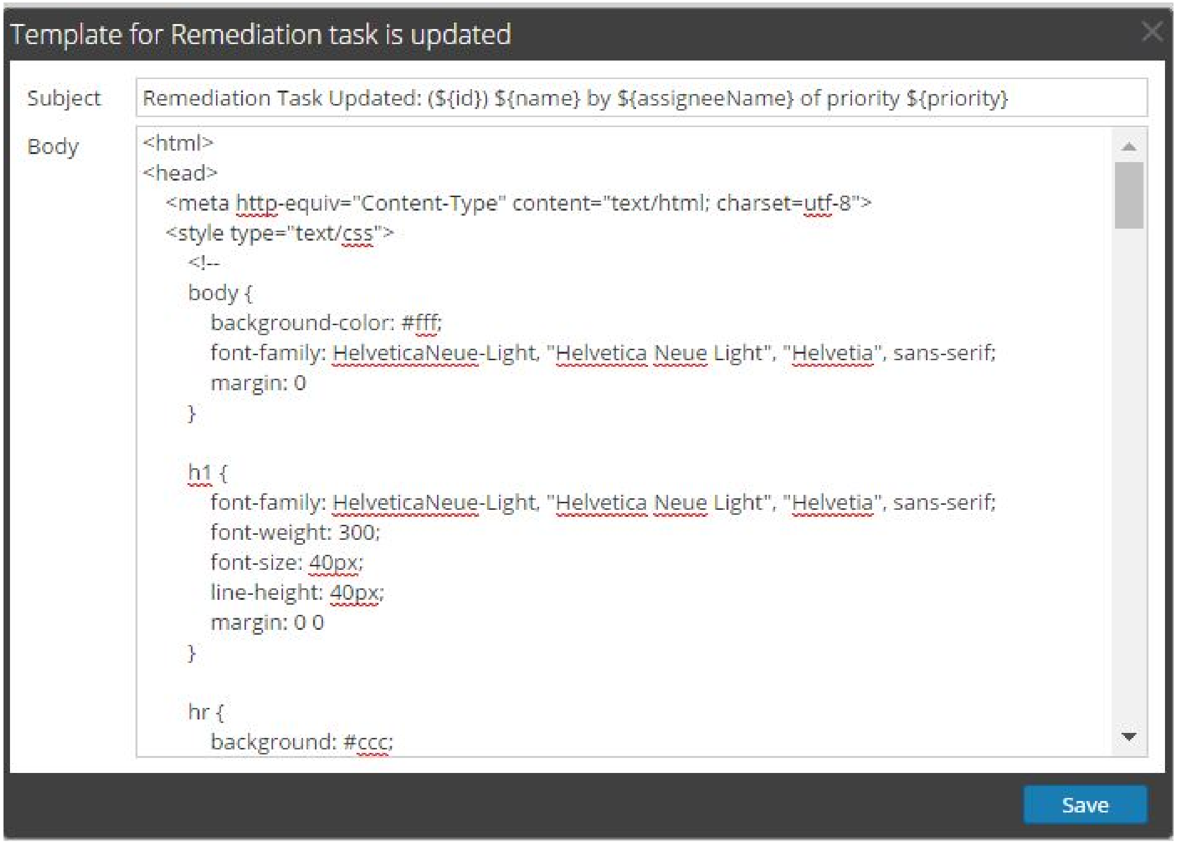
Body:

```
<html>
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
  <style type="text/css">
    <!--
    body {
      background-color: #fff;
      font-family: HelveticaNeue-Light, "Helvetica Neue Light", "Helvetia", sans-serif;
      margin: 0
    }

    h1 {
      font-family: HelveticaNeue-Light, "Helvetica Neue Light", "Helvetia", sans-serif;
      font-weight: 300;
      font-size: 40px;
      line-height: 40px;
      margin: 0 0
    }

    hr {
      background: #ccc;
```

The following figure shows you the remediation task updated template in the edit mode.



Subject: Remediation Task Updated: (${id}) ${name} by ${assigneeName} of priority ${priority}

Body:

```
<html>
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
  <style type="text/css">
    <!--
    body {
      background-color: #fff;
      font-family: HelveticaNeue-Light, "Helvetica Neue Light", "Helvetia", sans-serif;
      margin: 0
    }

    h1 {
      font-family: HelveticaNeue-Light, "Helvetica Neue Light", "Helvetia", sans-serif;
      font-weight: 300;
      font-size: 40px;
      line-height: 40px;
      margin: 0 0
    }

    hr {
      background: #ccc;
```

Note: You can edit the incident created template or remediation task updated template to include variables in the **Subject** field.
In case of an incident created template, you can use the following variables: id (String), assigneeName (String), priority (String), categories (Array).
In case of a remediation task updated template, you can use the following variables: id (String), assignee (String), priority (String), lastUpdated (Date).
This is intended for the user to get a quick context of the incident or remediation task.
Also, you can include array, date-time, custom-defined, and null type variables provided you use an appropriate free marker syntax to handle them.

5. Click **Apply** to save the Notification settings.

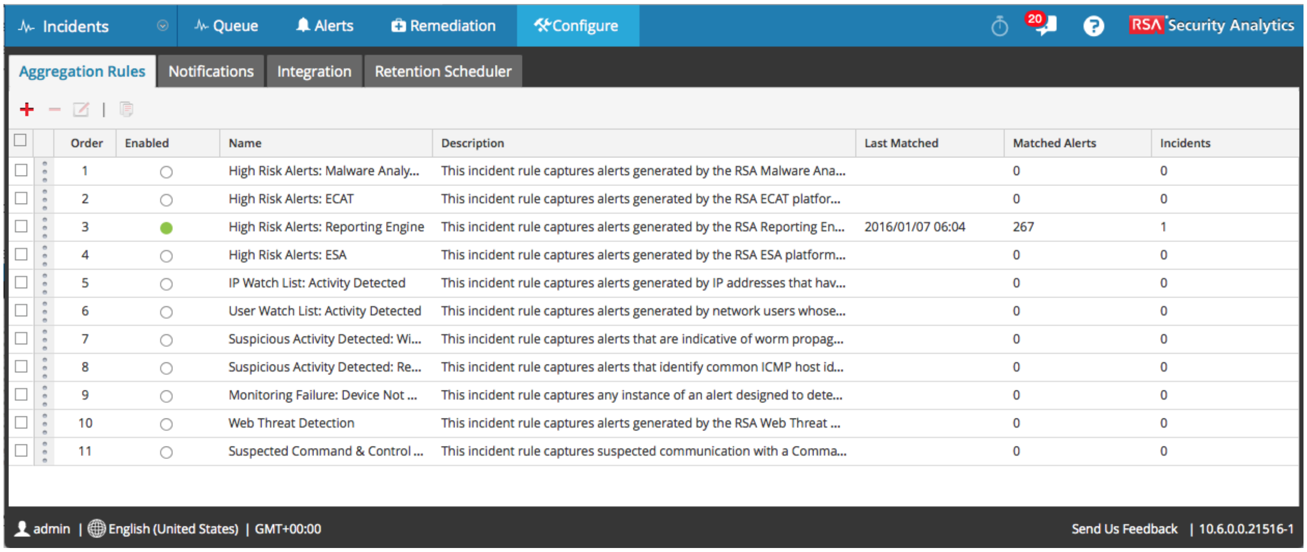
Create an Aggregation Rule

You can create aggregation rules with various criteria to automate the incident creation process. Alerts that meet the rule criteria are grouped together to form an incident. This is useful when you know a particular set of alerts can be grouped into an incident and you can set an aggregation rule that takes care of grouping the alerts instead of spending time in manually creating an incident and adding the alerts to that incident individually. To create incidents automatically you need to create an aggregation rule.

To create an aggregation rule:

1. In the **Security Analytics** menu, select **Incidents** > **Configure**.
2. Select **Aggregation Rules**.

   The **Aggregation Rules** view is displayed.



□	Order	Enabled	Name	Description	Last Matched	Matched Alerts	Incidents
□	1	○	High Risk Alerts: Malware Analy...	This incident rule captures alerts generated by the RSA Malware Ana...		0	0
□	2	○	High Risk Alerts: ECAT	This incident rule captures alerts generated by the RSA ECAT platfor...		0	0
□	3	●	High Risk Alerts: Reporting Engine	This incident rule captures alerts generated by the RSA Reporting En...	2016/01/07 06:04	267	1
□	4	○	High Risk Alerts: ESA	This incident rule captures alerts generated by the RSA ESA platform...		0	0
□	5	○	IP Watch List: Activity Detected	This incident rule captures alerts generated by IP addresses that hav...		0	0
□	6	○	User Watch List: Activity Detected	This incident rule captures alerts generated by network users whose...		0	0
□	7	○	Suspicious Activity Detected: Wi...	This incident rule captures alerts that are indicative of worm propag...		0	0
□	8	○	Suspicious Activity Detected: Re...	This incident rule captures alerts that identify common ICMP host id...		0	0
□	9	○	Monitoring Failure: Device Not ...	This incident rule captures any instance of an alert designed to dete...		0	0
□	10	○	Web Threat Detection	This incident rule captures alerts generated by the RSA Web Threat ...		0	0
□	11	○	Suspected Command & Control ...	This incident rule captures suspected communication with a Comma...		0	0

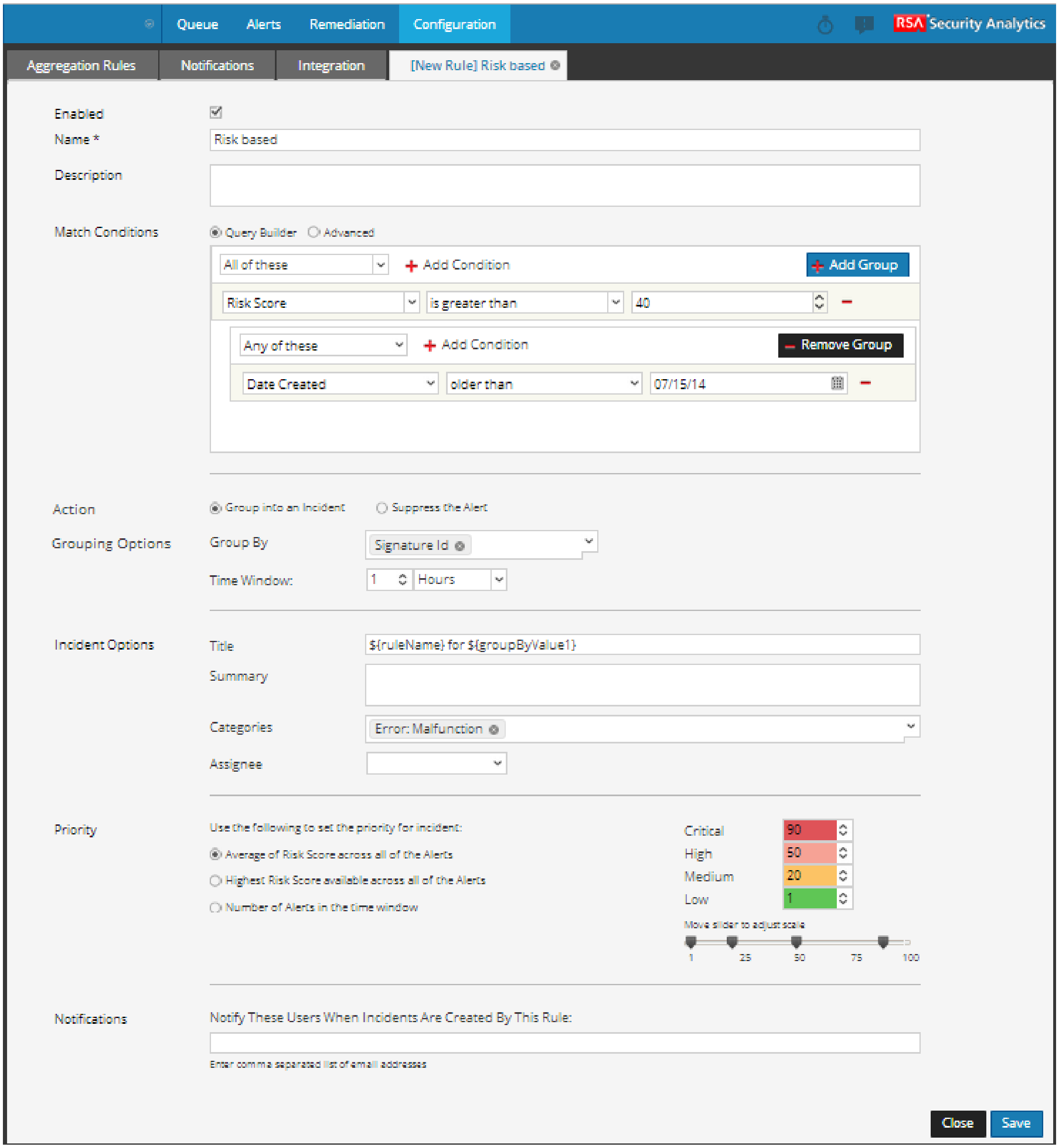
   A list of 9 pre-defined rules is displayed. You can do one of the following:

   - add a new rule
   - edit an existing rule
   - clone a rule

3. To add a new rule, select +.

   The **New Rule** tab is displayed.

   The example below shows grouping alerts into an incident based on the risk score.



Enabled ☑

Name * Risk based

Description

Match Conditions ● Query Builder ○ Advanced

All of these

Risk Score | is greater than | 40

Any of these

Date Created | older than | 07/15/14

Action ● Group into an Incident ○ Suppress the Alert

Grouping Options Group By: Signature Id

Time Window: 1 Hours

Incident Options Title: ${ruleName} for ${groupByValue1}

Summary

Categories: Error: Malfunction

Assignee

Priority Use the following to set the priority for incident:

● Average of Risk Score across all of the Alerts

○ Highest Risk Score available across all of the Alerts

○ Number of Alerts in the time window

Critical	90
High	50
Medium	20
Low	1

Move slider to adjust scale

1 25 50 75 100

Notifications Notify These Users When Incidents Are Created By This Rule:

Enter comma separated list of email addresses

4. Click **Save**.

   The rule is displayed in the **Aggregations Rules** view. The rule will be enabled and it starts creating incidents depending on the incoming alerts that are matched as per the criteria selected.

See Also:

- For details about various parameters that can be set as criteria for an aggregation rule, see New Rule Tab.
- For details on the parameter description and field description in the Aggregation Rules view, see Aggregation Rules Tab.

Set a Retention Period for Alerts and Incidents

Sometimes data privacy officers want to retain data for a certain period of time and then delete it. A shorter retention period frees up disk space sooner. In some cases, the retention period must be short. For example, laws in Europe state that sensitive data cannot be retained for more than 30 days. After 30 days, the data must be obfuscated or deleted.

Setting a retention period for data is an optional procedure. The time that Incident Management receives alerts and creates an incident determine when retention begins. Retention periods range from 30 to 365 days. If you set a retention period, one day after the period ends data is permanently deleted.

Retention is based on the time that IM receives the alerts and the incident creation time.

Caution: Data deleted after the retention period cannot be recovered.

When the retention period expires, the following data is **permanently deleted**:

- Alerts
- Incidents
- Remediation tasks
- Journal entries
- Attachments for the above

Logs track retention and manual deletion so you can see what has been deleted. To see im.log, click **Administration** > **Services**. Select an Incident Management service and click **View** > **Logs**. To see audit logs, go to /opt/rsa/im/logs on Security Analytics server.

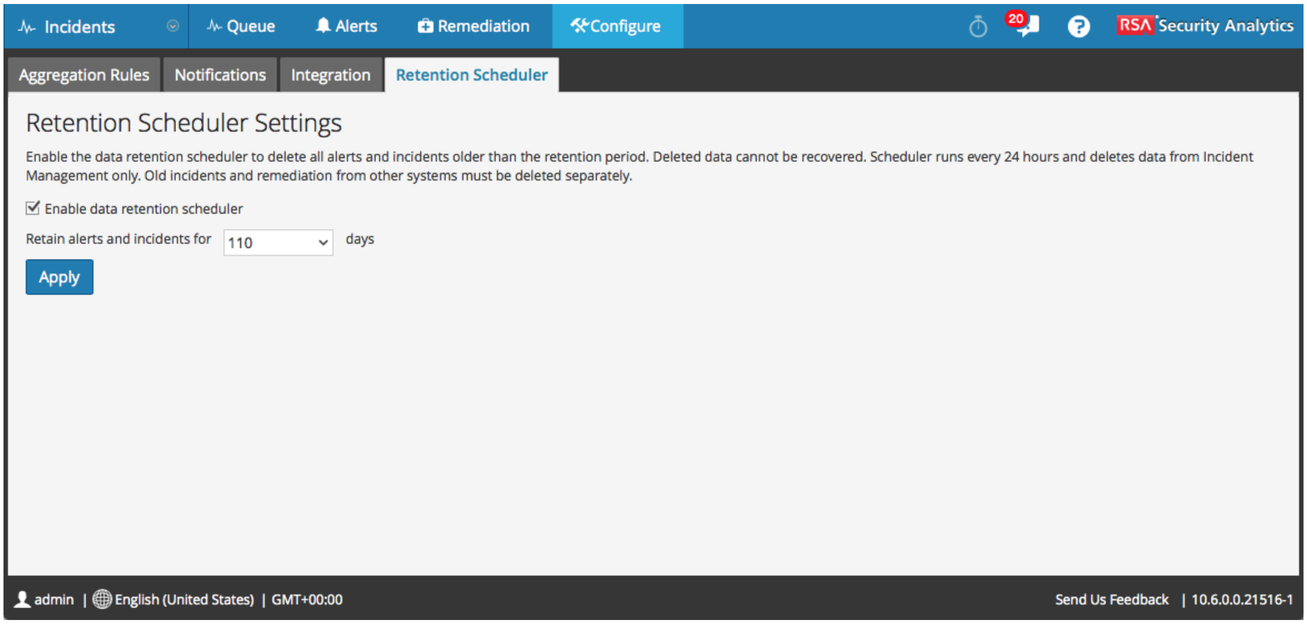
The feature does not apply to Archer or other third-party SOC tools. Alerts and incidents from other systems must be deleted separately.

Prerequisites

The Administrator role must be assigned to you.

Procedure

1. In the **Security Analytics** menu, select **Incidents** > **Configure**.
   The Configure panel is displayed with the Aggregation Rules tab open.
2. Select the **Retention Scheduler** tab.



Retention Scheduler Settings

Enable the data retention scheduler to delete all alerts and incidents older than the retention period. Deleted data cannot be recovered. Scheduler runs every 24 hours and deletes data from Incident Management only. Old incidents and remediation from other systems must be deleted separately.

☑ Enable data retention scheduler

Retain alerts and incidents for 110 days

Apply
admin | English (United States) | GMT+00:00
Send Us Feedback | 10.6.0.0.21516-1

3. Select **Enable data retention scheduler** to delete incidents and alerts older than the retention period.
   The scheduler runs every 24 hours at 23:00.
4. In the **Retain incidents and alerts for** field, select 30, 60, 90, 120 or 365 days or type any number.
5. Click **Apply**.

Result

Within 24 hours after the retention period ends, the scheduler permanently deletes all alerts and incidents older than the specified period from the Incident Management module. Journal entries and remediation tasks associated with the deleted incidents are also deleted.

Obfuscate Private Data

The Data Privacy Officer (DPO) role can identify meta keys that contain sensitive data and should display obfuscated data. This topic explains how the administrator maps those meta keys to display a hashed value instead of the actual value.

The following caveats apply to hashed meta values:

- Security Analytics supports two storage methods for hashed meta values, HEX (default) and string.
- When a meta key is configured to display a hashed value, all security roles see only the hashed value in the Incidents module.
- You use hashed values the same way you use actual values. For example, when you use a hashed value in rule criteria the results are the same as if you used the actual value.

This topic explains how to obfuscate private data in Incident Management. Refer to the **Data Privacy Management Overview** topic in the *Data Privacy Management* guide for additional information about data privacy.

Mapping File to Obfuscate Meta Keys

In the Incidents module, the mapping file for data obfuscation is data_privacy_map.js. In it you type an obfuscated meta key name and map it to the actual meta key name.

The following example shows the mappings to obfuscate data for two meta keys, ip.src and user.dst:

```
'ip.src.hash' : 'ip.src',
 'user.dst.hash' : 'user.dst'
```

You determine the naming convention for obfuscated meta key names. For example, ip.src.hash could be ip.src.private or ip.src.bin. You must choose one naming convention and use it consistently on all hosts.

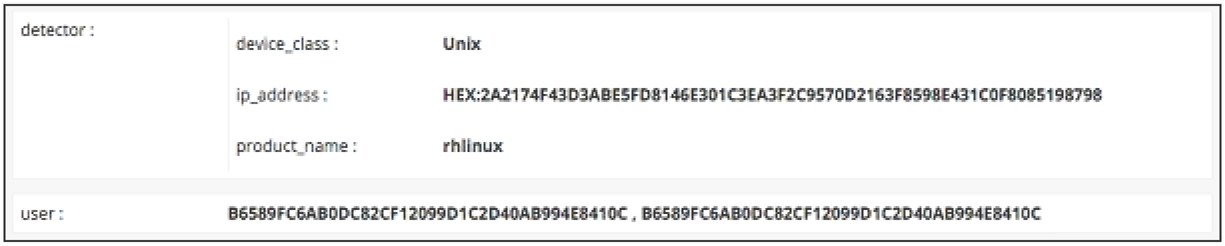
Prerequisites

- DPO role must specify which meta keys require data obfuscation.
- Administrator role must map meta keys for data obfuscation.

Procedure

1. Open the data privacy mapping file:
   /opt/rsa/im/scripts/normalize/data_privacy_map.js

2. In the `obfuscated_attribute_map` variable , type the name of a meta key to hold obfuscated data. Then map it to the meta key that does not contain obfuscated data according to this format:
   `'ip.src.hash' : 'ip.src'`
3. Repeat step 2 for every meta key that should display a hashed value.
4. Use the same naming convention as in step 2 and use it consistently on all hosts.
5. Save the file.
   All mapped meta keys will display hashed values instead of actual values.
   In the following graphic, hashed values display for the IP address and user:



detector :

device_class : Unix

ip_address : HEX:2A2174F43D3ABE5FD8146E301C3EA3F2C9570D2163F8598E431C0F8085198798

product_name : rhlinux

user : B6589FC6AB0DC82CF12099D1C2D40AB994E8410C , B6589FC6AB0DC82CF12099D1C2D40AB994E8410C

New alerts will display obfuscated data.

Note: Existing alerts still display sensitive data. This procedure is not retroactive.

System Integration

You can configure the integration settings so as to manage incidents in RSA Security Analytics or in RSA Archer Security Operations.

Topics

- Configure Integration Setting to Manage Incidents in Security Analytics
- Configure Integration Setting to Manage Incidents in RSA Archer Security Operations

Configure Integration Setting to Manage Incidents in Security Analytics

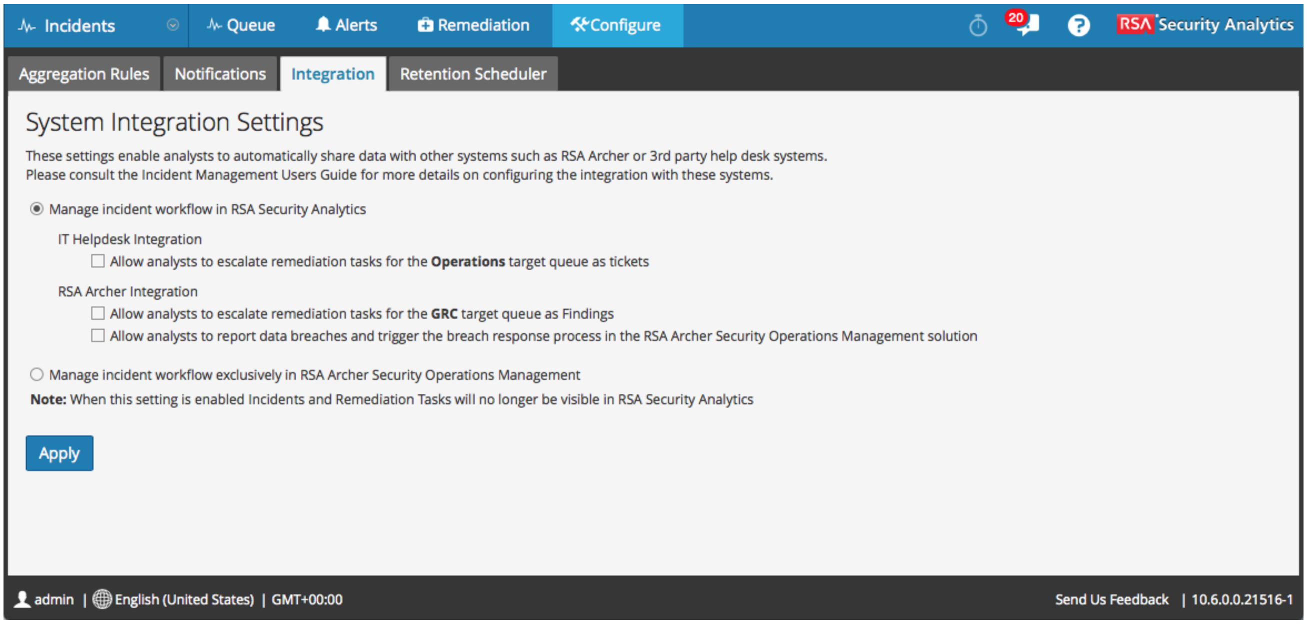
You have to configure system integration settings to manage incidents in Security Analytics. You can enable integration with:

- IT helpdesk ticketing system that helps you push remediation tasks as helpdesk tickets.
- RSA Archer that helps you to push the remediation tasks to the Archer target queue and to report data breaches and track them through the breach response process in the RSA Security Operations Management solution.

To configure integration settings to manage incidents in Security Analytics:

1. In the **Security Analytics** menu, select **Incidents > Configure**.
2. Select **Integration**.

   The System Integration Settings view is displayed.



System Integration Settings

These settings enable analysts to automatically share data with other systems such as RSA Archer or 3rd party help desk systems.
Please consult the Incident Management Users Guide for more details on configuring the integration with these systems.

● Manage incident workflow in RSA Security Analytics

IT Helpdesk Integration

□ Allow analysts to escalate remediation tasks for the **Operations** target queue as tickets

RSA Archer Integration

□ Allow analysts to escalate remediation tasks for the **GRC** target queue as Findings
□ Allow analysts to report data breaches and trigger the breach response process in the RSA Archer Security Operations Management solution

○ Manage incident workflow exclusively in RSA Archer Security Operations Management

Note: When this setting is enabled Incidents and Remediation Tasks will no longer be visible in RSA Security Analytics

3. Select **Manage Incident Workflow in RSA Security Analytics**.
4. Select one or more of the following options:

   - **Allow Analysts to escalate remediation tasks for the Operations target queue as tickets** - This enables you to push remediation tasks as help desk tickets and track them to closure.

- **Allow Analysts to escalate remediation tasks for the GRC target queue as Findings -** This enables you to escalate and push remediation tasks to the Archer target queue with additional information that helps in tracking it to closure.
- **Allow Analysts to report data breaches and trigger the breach response process in the RSA Security Operations Management solution -** This enables you to report a data breach and track it through the breach response process in the RSA Security Operations Management solution

5. Select **Apply** to save the configuration settings.

Configure Integration Setting to Manage Incidents in RSA Archer Security Operations

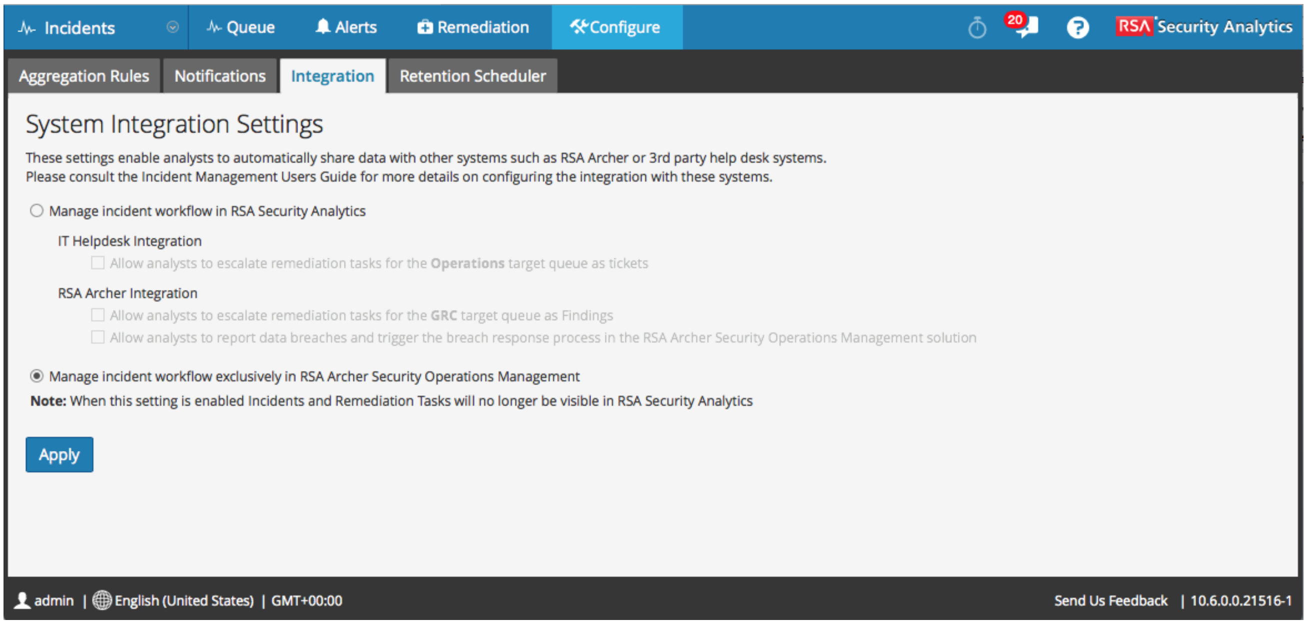
You have to configure system integration settings to manage incident workflow in RSA Archer Security Operations. When this setting is enabled, Incidents and Remediation Tasks will no longer be visible in RSA Security Analytics.

For the versions of Archer SecOps that are compatible with Security Analytics refer to the *RSA Archer Integration Guide*.

To configure integration settings to manage incident workflow in RSA Archer Security operations:

1. In the **Security Analytics** menu, select **Incidents** > **Configure**.
2. Click the **Integration** tab.

   The System Integration Settings view is displayed.



System Integration Settings

These settings enable analysts to automatically share data with other systems such as RSA Archer or 3rd party help desk systems.
Please consult the Incident Management Users Guide for more details on configuring the integration with these systems.

○ Manage incident workflow in RSA Security Analytics

IT Helpdesk Integration

□ Allow analysts to escalate remediation tasks for the **Operations** target queue as tickets

RSA Archer Integration

□ Allow analysts to escalate remediation tasks for the **GRC** target queue as Findings

□ Allow analysts to report data breaches and trigger the breach response process in the RSA Archer Security Operations Management solution

● Manage incident workflow exclusively in RSA Archer Security Operations Management

Note: When this setting is enabled Incidents and Remediation Tasks will no longer be visible in RSA Security Analytics

Apply

3. Select **Manage Incident workflow exclusively in RSA Archer Security Operations Management.**
4. Select **Apply** to save the configuration settings.

Incident Management Reference Information

The Incident Management module user interface provides access to Security Analytics incident management functions. This topic contains descriptions of the user interface as well as other reference information to help users understand the functions of Incident Management.

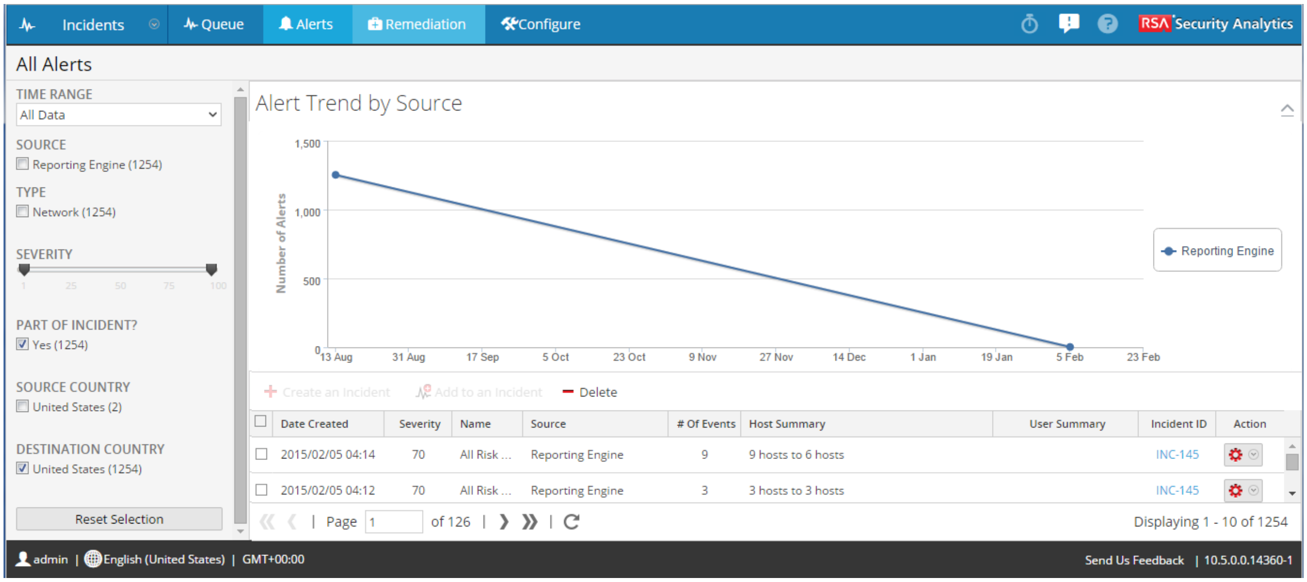
Topics

- Alerts View
- Configure View
- Incident Queue View
- Remediation View

Alerts View

This topic describes how to access the Alerts view, details about the Alerts view, and understanding various aspects of alerts. In the Alerts view you can browse through various alerts, filter them, and group them to create incidents.

To access the Alerts view, in the **Security Analytics** menu, select **Incidents** > **Alerts**. The All Alerts view is displayed. You can customize the Alerts view to view alerts as per your requirement.



☐	Date Created	Severity	Name	Source	# Of Events	Host Summary	User Summary	Incident ID	Action
☐	2015/02/05 04:14	70	All Risk ...	Reporting Engine	9	9 hosts to 6 hosts		INC-145	
☐	2015/02/05 04:12	70	All Risk ...	Reporting Engine	3	3 hosts to 3 hosts		INC-145	

Features

The Alerts view offers several details and commands to help customize the view and display alerts.

Alerts View Details

The options panel in the All Alerts view displays various parameters that can be used to customize the alert display.

The following table describes the various parameters that you can select to filter the alerts and customize the view. The filter parameters you choose to filter the alerts are persisted and retained when you navigate away from the present view to switch between tabs, sessions or when you navigate to the details screen. The Reset Selection option enables you to reset the filter options to the default value.

Parameter	Description
TIME RANGE	Select a time range to view alerts in that time range. For example: • Select **Last 24 Hours** to view alerts triggered in the last 24 hours. • Select **All Data** to view alerts triggered from the time the service was added. • Select **Custom** and provide a date range to view alerts triggered in that time frame.
SOURCE	Indicates the number of Alerts categorized depending on their sources. For example, RSA ECAT(86) indicates there are 86 alerts triggered by RSA ECAT. Select one or multiple sources to view alerts triggered by the selected sources. For example, to view ECAT Alerts only, select RSA ECAT as the source.
TYPE	Indicates the type of events in the alert, for example, logs, network sessions, and so on.
SEVERITY	Indicates the severity of the alerts. Select a value to view the alerts of the required severity. For example, to view alerts of severity 75, select 75 as the severity level.
PART OF INCIDENT?	Indicates the number of Alerts categorized depending whether they belong to an incident or not. For example, Yes(180) indicates there are 180 alerts that are part of incident. Select **Yes** to view alerts that are part of an incident. Select **No** to view alerts that are not part of any incident.
SOURCE COUNTRY	If geo-ip is enabled on the Decoder, filters on the country tagged on the source device in an event within the Alert.
DESTINATION COUNTRY	If geo-ip is enabled on the Decoder, filters on the country tagged on the destination device in an event within the Alert.

Parameter	Description
	Resets filter options to default values.

The top half of the Alert panel displays the graphical representation of the trend of alerts over time (grouped by each source) that match the filter criteria as per the parameters chosen.

Alert Details

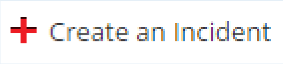
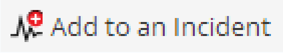
The bottom half of the Alert panel displays the alert details. The following table describes the various alert details.

Field	Description
Date Created	Displays the date when the alert was created.
Severity	Displays the severity of the alert. The values are from 1 through 100.
Name	Displays the name of the alert.
Source	Displays the source of the alert. The source of the alerts can be ECAT, Malware Analytics, ESA, Investigator service or Reporting Engine.
# Of Events	Indicates the number of events contained within an alert. **Note:** This varies depending on the source of the alert. For example, ECAT and MA alerts always have one Event. For certain types of alerts, a high number of events may mean that the alert is more risky.
Host Summary	Displays details of the host like host name from where the alert was triggered. The details may include information about the source and/or destination devices in an Alert. Some alerts may describe events across more than one device.
User Summary	Displays the summary of the user or users associated with the events in the Alert.
Incident ID	Displays the Incident ID of the incident of which the alert belongs to. If there is no incident ID it implies that the alert does not belong to any incident and you can create an incident to include this alert or the alert can be added to an existing incident.

Field	Description
Action	Allows you to investigate the alert further. The available options to investigate further are different for different types of Alerts. For example: For an ECAT alert the available option is **View ECAT Analysis**. It allows you to view the host analysis in the ECAT client, if you have it installed on your client machine. For an ESA or Reporting Engine the available options are **Investigate Events**, **Investigate Device IP Address**, **Investigate Source IP Address**, and **Investigate Destination IP Address**. It allows you to view the events in the Investigator view, or view similar Events (for example. by the same source or destitution IP address). For a Malware Analytics the available option is **View Malware Analysis**. It allows you to view the Event details from the malware analysis.

Options

The bottom half of the Alert panel provides you options to perform various operations. The table describes the various commands available.

Command	Action
 + Create an Incident	Select this to create an incident. Refer to Create an Incident Manually.
 Add to an Incident	Select this to add the selected alert to an existing incident. Refer to Add Alerts to an Existing Incident.
— Delete	Select this to delete alerts. Refer to Delete Alerts.

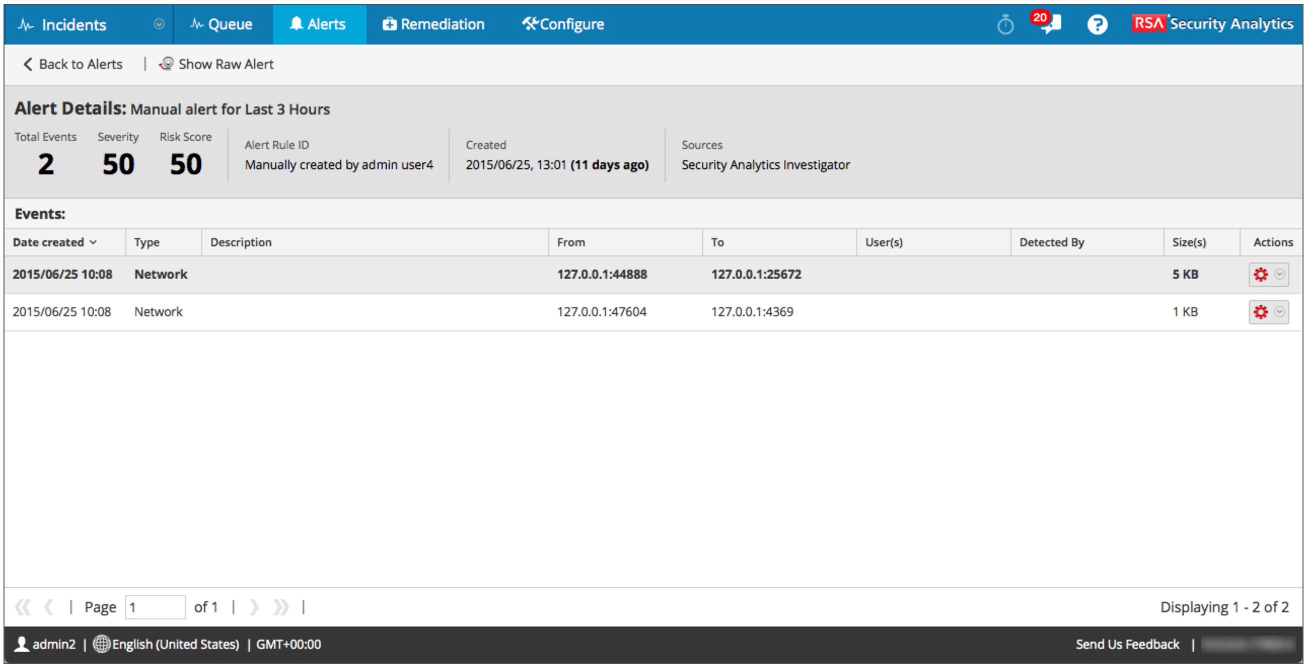
Alerts Details View

In the Alerts Details view, you can see the details of an alert.

To access the Alerts Details view:

1. 1. In the **Security Analytics** menu, select **Incidents** > **Alerts**.
2. Double-click an alert.

   The Alert Details view is displayed.



Alert Details: Manual alert for Last 3 Hours

Total Events	Severity	Risk Score	Alert Rule ID	Created	Sources
2	50	50	Manually created by admin user4	2015/06/25, 13:01 **(11 days ago)**	Security Analytics Investigator

Events:

Date created	Type	Description	From	To	User(s)	Detected By	Size(s)	Actions
2015/06/25 10:08	**Network**		**127.0.0.1:44888**	**127.0.0.1:25672**			**5 KB**	
2015/06/25 10:08	Network		127.0.0.1:47604	127.0.0.1:4369			1 KB	

Page 1 of 1
Displaying 1 - 2 of 2
admin2 | English (United States) | GMT+00:00
Send Us Feedback | [redacted]

Related procedures are available in Filter Alerts.

Features

The following table lists the parameters displayed in the Alerts Details view.

Parameter	Description
Total Events	Displays the total number of events.
Severity	Displays the level of severity.
Risk Score	Displays the level of risk.
Alert Rule ID	Displays how and by whom the alert was created.

Parameter	Description
Created	Displays details about the date and time when the task was created.
Sources	Displays the original source.

Toolbar

The following table lists the operations that can be performed in the Alerts Details view.

Parameter	Description
Back to Alerts	Allows you to navigate back to the Alerts View.
Show Raw Alert	Displays Raw Alert Data details.
View Event Details	Displays details of the event including: related links, data, destination, and source.
View Original Event	Displays Event Reconstruction and details on the service, id, type, source, destination, and service.

Configure View

The Configure view enables you to configure the system's Incident Management functionality. You can configure notification settings, third party system integration for incident management, and aggregation rules to automate the incident management workflow for automatically creating incidents.

The Configure view has three subviews for the various functions.

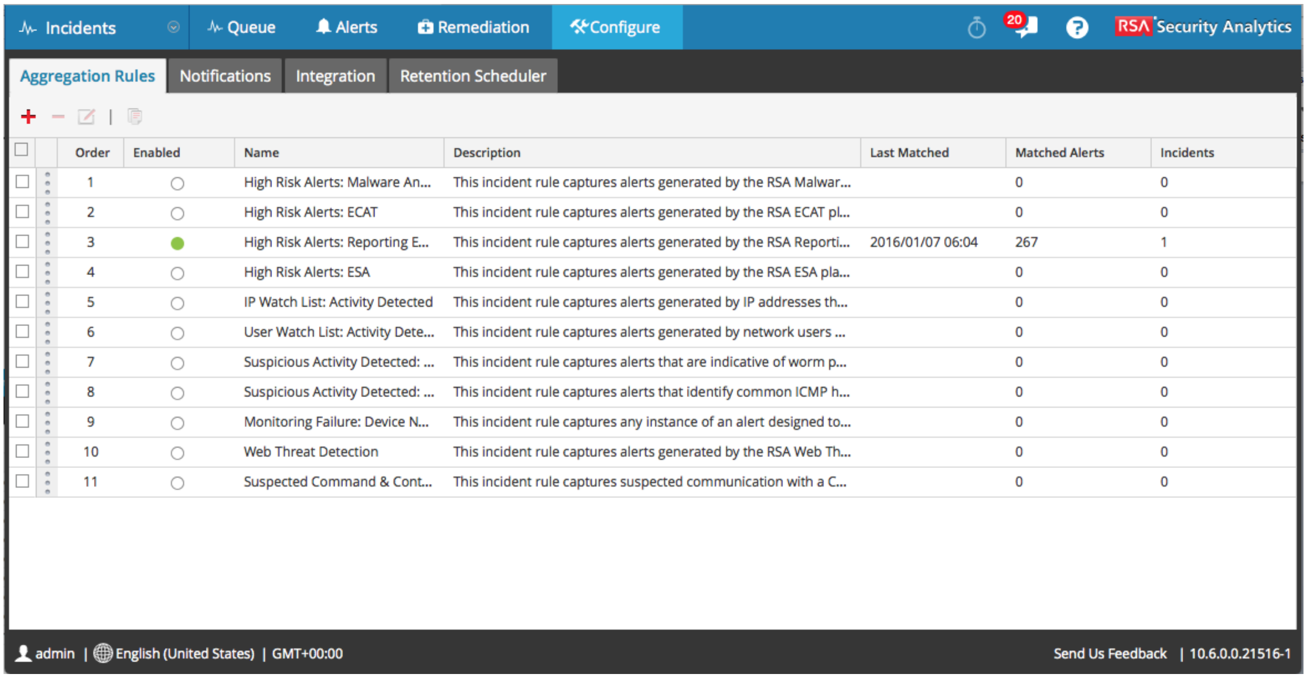
Topics

- Aggregation Rules Tab
- Integration Tab
- Notifications Tab
- Retention Scheduler Tab

Aggregation Rules Tab

This topic covers information of parameters required in creating and managing aggregation rules for automating the incident creation process as part of the incident management workflow.

To access the Aggregation Rules view, in the **Security Analytics** menu, select **Incidents** > **Configure** > **Aggregation Rules**. The Aggregation Rules view is displayed.



□	Order	Enabled	Name	Description	Last Matched	Matched Alerts	Incidents
□	1	○	High Risk Alerts: Malware An...	This incident rule captures alerts generated by the RSA Malwar...		0	0
□	2	○	High Risk Alerts: ECAT	This incident rule captures alerts generated by the RSA ECAT pl...		0	0
□	3	●	High Risk Alerts: Reporting E...	This incident rule captures alerts generated by the RSA Reporti...	2016/01/07 06:04	267	1
□	4	○	High Risk Alerts: ESA	This incident rule captures alerts generated by the RSA ESA pla...		0	0
□	5	○	IP Watch List: Activity Detected	This incident rule captures alerts generated by IP addresses th...		0	0
□	6	○	User Watch List: Activity Dete...	This incident rule captures alerts generated by network users ...		0	0
□	7	○	Suspicious Activity Detected: ...	This incident rule captures alerts that are indicative of worm p...		0	0
□	8	○	Suspicious Activity Detected: ...	This incident rule captures alerts that identify common ICMP h...		0	0
□	9	○	Monitoring Failure: Device N...	This incident rule captures any instance of an alert designed to...		0	0
□	10	○	Web Threat Detection	This incident rule captures alerts generated by the RSA Web Th...		0	0
□	11	○	Suspected Command & Cont...	This incident rule captures suspected communication with a C...		0	0

admin | English (United States) | GMT+00:00 Send Us Feedback | 10.6.0.0.21516-1

Features

The Aggregation Rules tab consists of a grid and toolbar.

Aggregation Rules Grid

The following table lists the parameters that need to be provided for creating new aggregation rules.

Parameter	Description
Order	Denotes the order in which the rule is placed. The rule order determines which rule takes effect if the criteria for multiple rules match the same alert.
Name	Displays the name of the rule.
Enabled	Denotes whether the rule is enabled or not. The ● specifies the rule is enabled.

Parameter	Description
Description	Displays the description of the rule.
Last Run	Displays the time when the rule was last run. This value is reset once a week.
Matched Alerts	Displays the number of matched alerts. This value is reset once a week. To change the setting, see the **Set Counter for Matched Alerts and Incidents** topic in the *Incident Management Configuration Guide*.
Incidents	Displays the number of incidents created by the rule. This value is reset once a week. To change the setting, see the **Set Counter for Matched Alerts and Incidents** topic in the *Incident Management Configuration Guide*.

Toolbar

The following table lists the operations that can be performed in the Aggregation Rules view.

Parameter	Description
+	Allows you to add a new rule.
✎	Allows you to edit a rule.
−	Allows you to delete a rule.
🗐	Allows you to duplicate a rule.

New Rule Tab

This topic covers information of parameters required in creating a new rule.

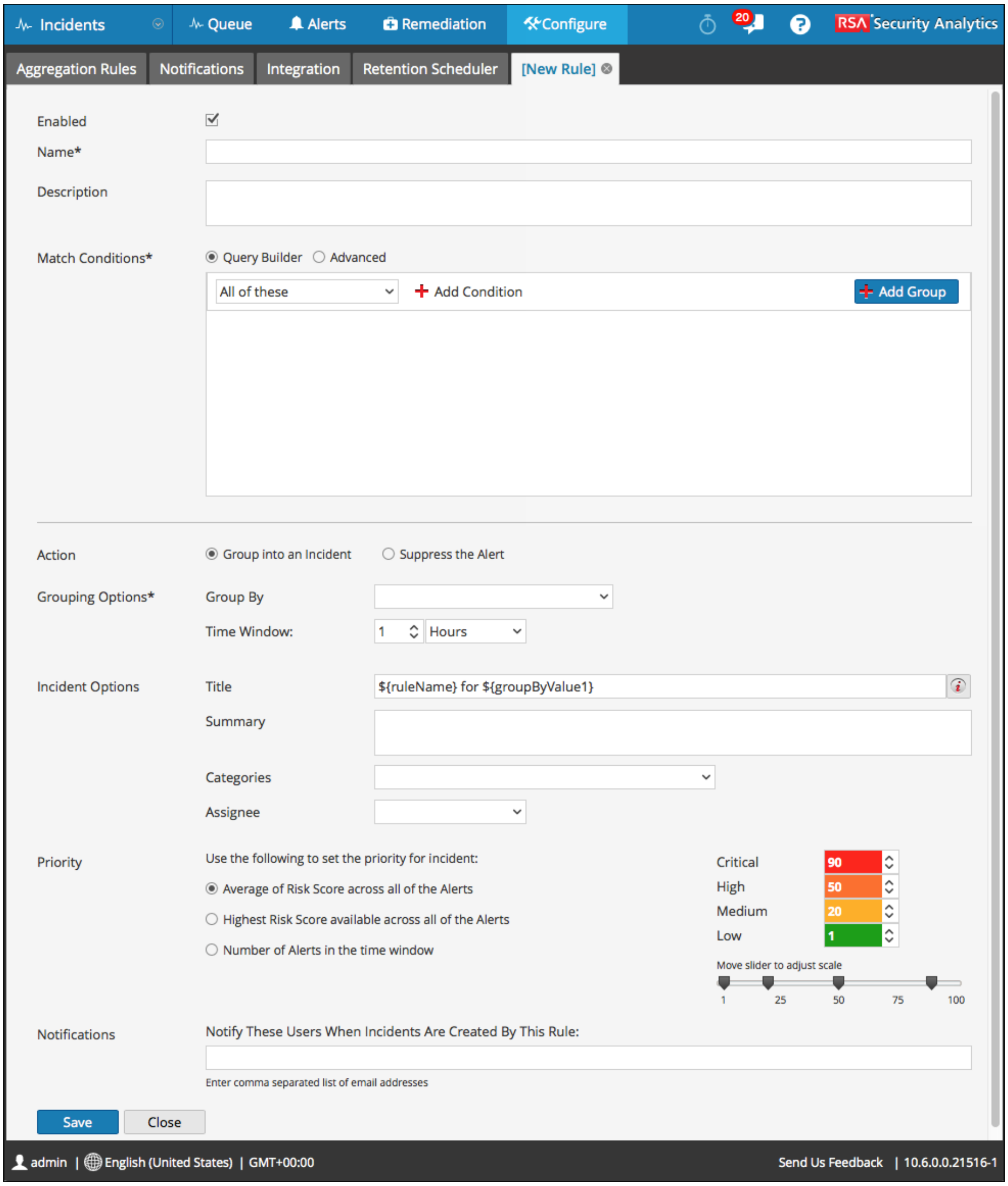
To access the New Rule tab view:

1. In the **Security Analytics** menu, select **Incidents** > **Configure** > **Aggregation Rules**.

   The Aggregation Rules view is displayed.

2. Click +.

   The **New Rule** tab is displayed.



Enabled ☑

Name*

Description

Match Conditions* ● Query Builder ○ Advanced

All of these

Action ● Group into an Incident ○ Suppress the Alert

Grouping Options* Group By

Time Window: 1 Hours

Incident Options Title ${ruleName} for ${groupByValue1}

Summary

Categories

Assignee

Priority Use the following to set the priority for incident:

● Average of Risk Score across all of the Alerts

○ Highest Risk Score available across all of the Alerts

○ Number of Alerts in the time window

Critical	90
High	50
Medium	20
Low	1

Move slider to adjust scale

1 25 50 75 100

Notifications Notify These Users When Incidents Are Created By This Rule:

Enter comma separated list of email addresses

The New Rule view offers several fields in which you can customize a new rule.

The following table lists the parameters that need to be provided for creating new aggregation rules.

Parameter	Description
Enabled	Select to enable the rule.
Name*	Name of the rule. This is a required field.
Description	A description for the rule to give an idea about what alerts get aggregated.
Match Conditions*	**Query Builder** - Select if you want to build a query with various conditions that can be grouped. You can also have nested groups of conditions. Match Conditions - You can set the value to **All of these**, **Any of these**, or **None of these**. Depending on what you select the the criteria types specified in the Conditions and Group of conditions are matched to group the alerts. **For example**, if you set the match condition to All of these, alerts that match the criteria mentioned in the Conditions and Group Conditions are grouped into one incident. Add a Condition to be matched by clicking <> Add a Group of Conditions by clicking <> and adding conditions by clicking <> You can include multiple Conditions and Groups of Conditions that can be matched as per criteria set and group the incoming alerts into incidents.
	Advanced - Select if you want to add an advanced query builder. You can add a specific condition that needs to be matched as per the matching option selected. **For example:** you can type the criteria builder format **{"$and": [{"alert.severity" : {"$gt":4}}]}** to group alerts that have severity greater than 4. For advanced syntax, refer to http://docs.mongodb.org/manual/reference/operator/query/ or http://docs.mongodb.org/manual/reference/method/db.collection.find/
Action	**Group into an Incident** - If enabled, the alerts that match the criteria set are grouped into an alert. **Suppress the Alert** - If enabled, the alerts that match the criteria are suppressed.

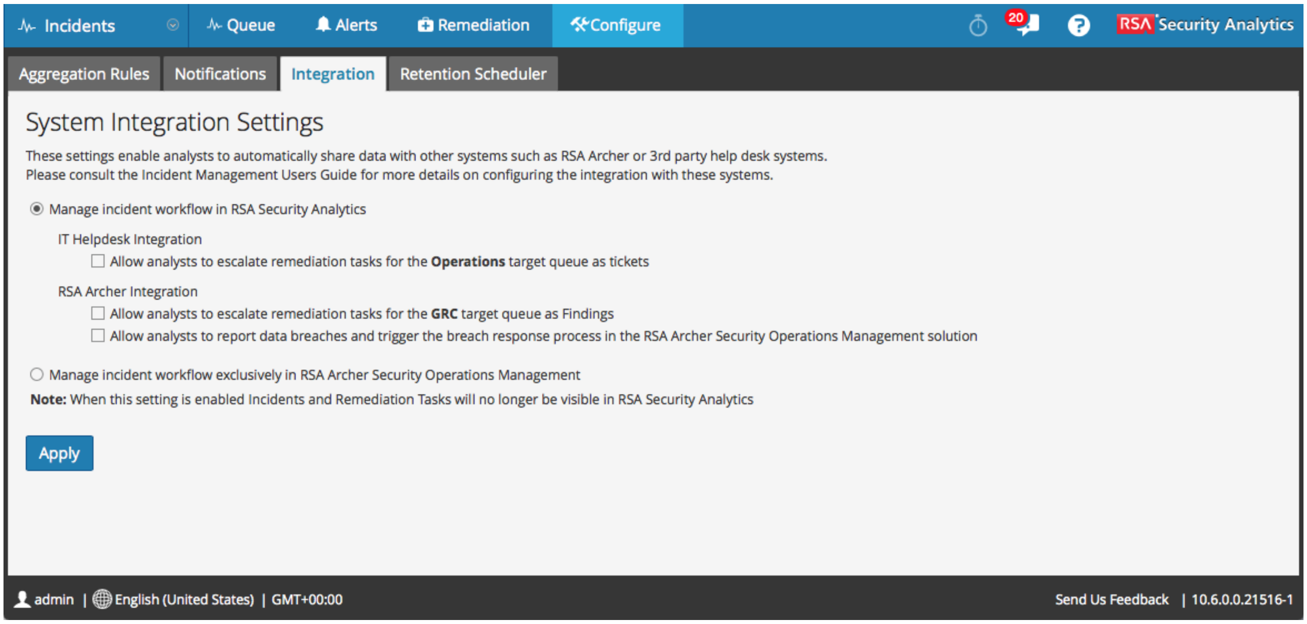
Parameter	Description
Grouping Options*	**Group By:** The criteria to group the alerts as per the specified category. You can group the alerts with no attributes (all matching Alerts grouped together), 1 attribute, or 2 attributes. Grouping on an attribute means that all matching Alerts containing the same value for that attribute are grouped together in the same Incident. **Time Window:** The time range specified to group alerts. For example if the time window is set to 1 hour, all alerts that match the criteria set in Group By field and that arrive within an hour of each other are grouped into an incident.
Incident Options	**Title -** (Optional) Title of the incident. You can provide placeholders based on the attributes you grouped. Placeholders are optional. If you do not use placeholders, all Incidents created by the rule will have the same title. For example, if you grouped them according to the source, you can name the resulting Incident as Alerts for **${groupByValue1}**, and the incident for all alerts from ECAT would be named **Alerts for ECAT**.
	Summary - (Optional) Summary of the incident.
	Categories - (Optional) Category of the incident created. An incident can be classified using more than one category.
	Assignee - (Optional) Name of the assignee to whom the incident is assigned to.
Priority	**Average of Risk Score across all of the Alerts** - Takes the average of the risk scores across all the alerts to set the priority of the incident created. **Highest Risk Score available across all of the Alerts** - Takes the highest score available across all the alerts to set the priority of the incident created. **Number of Alerts in the time window** - Takes the count of the number of alerts in the time window selected to set the priority of the incident created. Move the slider to adjust the scale that sets the priority level of the incident.
Notifications	A set of email addresses of the users to be notified when incidents are created by this rule.

Integration Tab

The Integration tab enables you to configure the System Integration settings, which allow analysts to automatically share data with other systems, such as RSA Archer or 3rd party help desk systems.

To access this tab, select **Incidents > Configure** in the **Security Analytics** menu, then select the **Integration** tab.

The Integration tab consists of the System Integration Settings panel, where you can choose where to manage incident workflow and set integration permissions for analysts. The following figure shows the Integration tab.



System Integration Settings

These settings enable analysts to automatically share data with other systems such as RSA Archer or 3rd party help desk systems.
Please consult the Incident Management Users Guide for more details on configuring the integration with these systems.

● Manage incident workflow in RSA Security Analytics

IT Helpdesk Integration

□ Allow analysts to escalate remediation tasks for the **Operations** target queue as tickets

RSA Archer Integration

□ Allow analysts to escalate remediation tasks for the **GRC** target queue as Findings

□ Allow analysts to report data breaches and trigger the breach response process in the RSA Archer Security Operations Management solution

○ Manage incident workflow exclusively in RSA Archer Security Operations Management

Note: When this setting is enabled Incidents and Remediation Tasks will no longer be visible in RSA Security Analytics

Apply

The following table describes the configuration parameters.

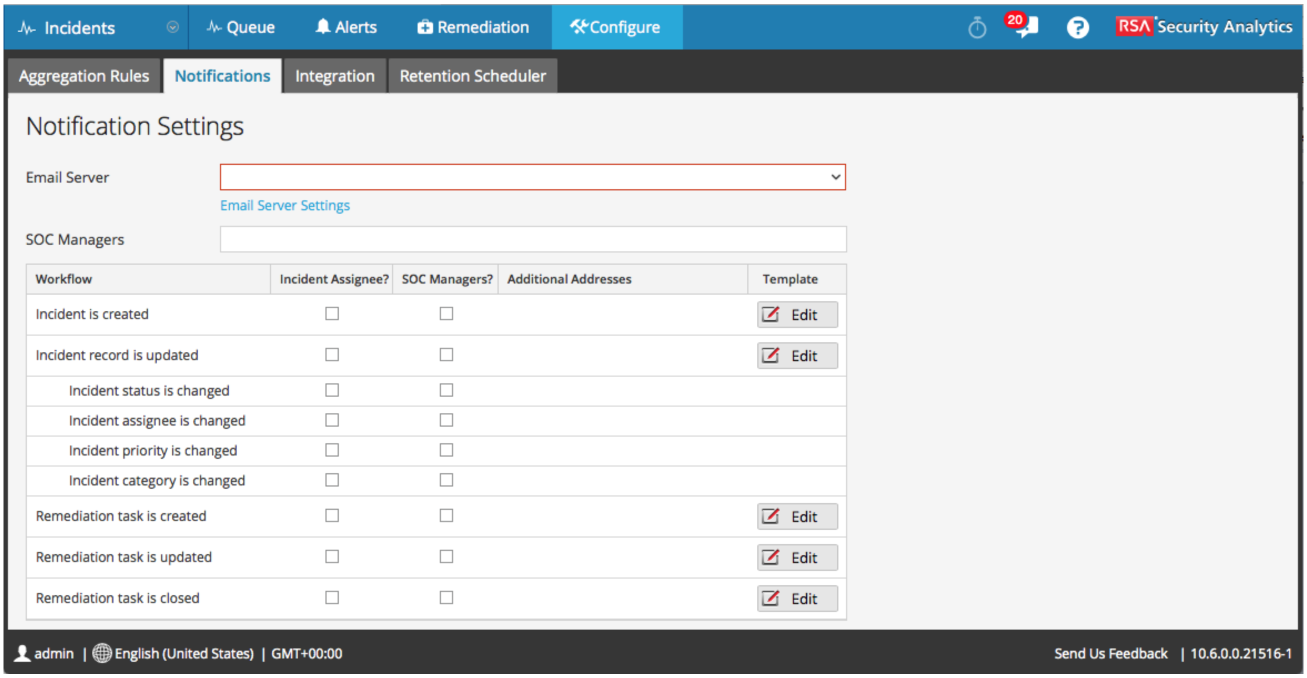
Parameter	Description
Manage incident workflow in Security Analytics	Enables incident workflow management in Security Analytics. Selecting this option disables the **Manage incident workflow exclusively in RSA Archer Security Operations Management**.
Allow analysts to escalate remediation tasks for the **Operations** target queue as tickets	Enables you to push remediation tasks as help desk tickets and track them to closure.

Parameter	Description
Allow analysts to escalate remediation tasks for the **GRC** target queue as Findings	Enables you to escalate and push remediation tasks to the Archer target queue with additional information that helps in tracking it to closure.
Allow analysts to report data breaches and trigger the breach response process in the RSA Archer Security Operations Management solution	Enables you to report a data breach and track it through the breach response process in the RSA Archer Security Operations Management solution.
Manage incident workflow exclusively in RSA Archer Security Operations Management	Disables incident workflow management outside of RSA Archer Security Operations Management. Incidents and Remediation tasks are no longer visible in RSA Security Analytics, and the **Manage incident workflow in Security Analytics** options are unavailable.

Notifications Tab

In this view you can set notifications for various operations that are performed through out the incident management workflow.

To access the Notification Settings view, in the **Security Analytics** menu, select **Incidents** > **Configure** > **Notifications**. The Notification Settings view is displayed.



Notification Settings

Email Server

Email Server Settings

SOC Managers

Workflow	Incident Assignee?	SOC Managers?	Additional Addresses	Template
Incident is created	□	□		Edit
Incident record is updated	□	□		Edit
Incident status is changed	□	□		
Incident assignee is changed	□	□		
Incident priority is changed	□	□		
Incident category is changed	□	□		
Remediation task is created	□	□		Edit
Remediation task is updated	□	□		Edit
Remediation task is closed	□	□		Edit

The Notifications tab consists of the Notification Settings panel.

The following table lists the parameters that need to be enabled for notification settings.

Parameter	Description
Email Server	The Email server address to be configured to send out mail notifications for the notification settings enabled.
Configure email or distribution list	Click this to configure an email server if the email server is not listed in the Email server drop-down list.
SOC Managers	SOC Manager email addresses to which the notification mail is sent for the selected operations.
Workflow	The workflow in which a notification is sent if enabled.

Parameter	Description
Incident Assignee?	Select if you want a mail notification to be sent for the corresponding workflow whenever an incident is assigned.
SOC Managers?	Select if you want a mail notification to be sent to the SOC managers for the corresponding workflow.
Additional Addresses	Additional addresses to which you want mail notifications to be sent for the corresponding workflow.
Template	Click **Edit** to modify the template for the selected workflow.
Apply	Click **Apply** to save the settings applied.

Retention Scheduler Tab

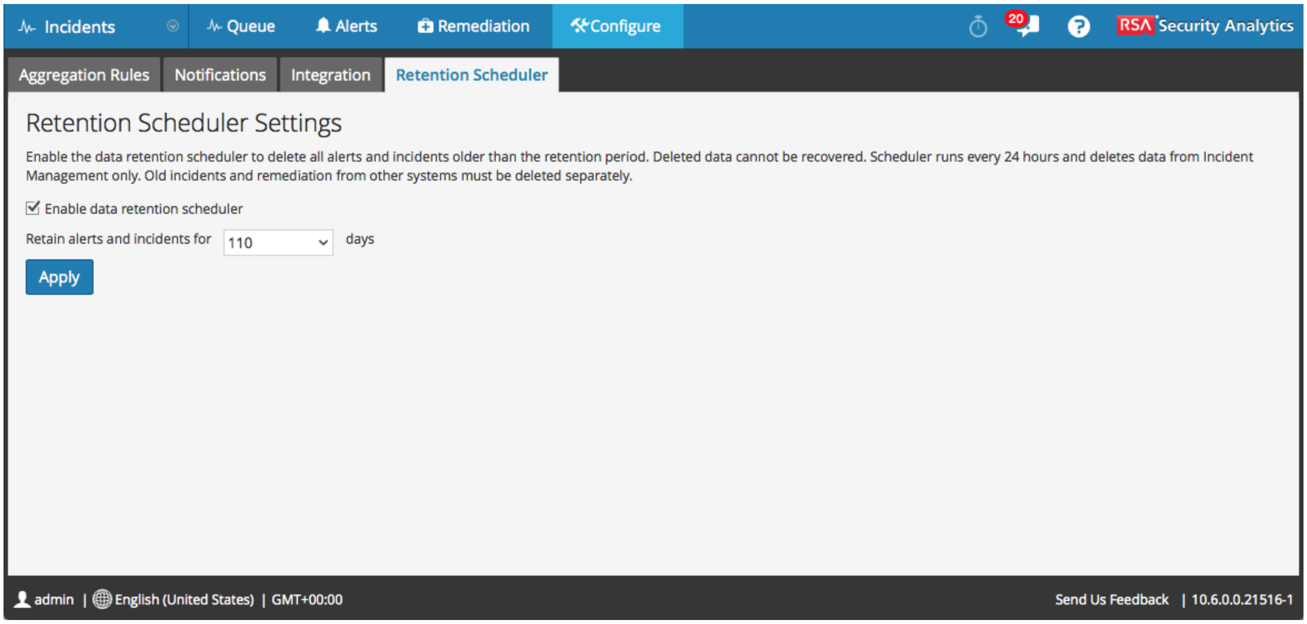
The settings in the Retention Scheduler tab allow you to specify a retention period for alerts and incidents.

To access the Retention Scheduler tab:

1. In the **Security Analytics** menu, select **Incidents > Configure**.

   The Configure panel opens to the Aggregation Rules tab by default.

2. Select the **Retention Scheduler** tab.



Retention Scheduler Settings

Enable the data retention scheduler to delete all alerts and incidents older than the retention period. Deleted data cannot be recovered. Scheduler runs every 24 hours and deletes data from Incident Management only. Old incidents and remediation from other systems must be deleted separately.

☑ Enable data retention scheduler

Retain alerts and incidents for 110 days

The Retention Scheduler tab has these features:

Feature	Description
Number of days	Specifies how long to keep alerts and incidents before they get deleted.
Enable	Deletes alerts and incidents when the retention period ends.
Apply	Puts the settings into effect immediately.

Incident Queue View

In the Incident Queue view, you can see a list of all incidents assigned and unassigned. You can manage and track these incidents to closure.

To access the Incident Queue tab, in the **Security Analytics** menu, select **Incidents** > **Queue.** A queue of all incidents is displayed.

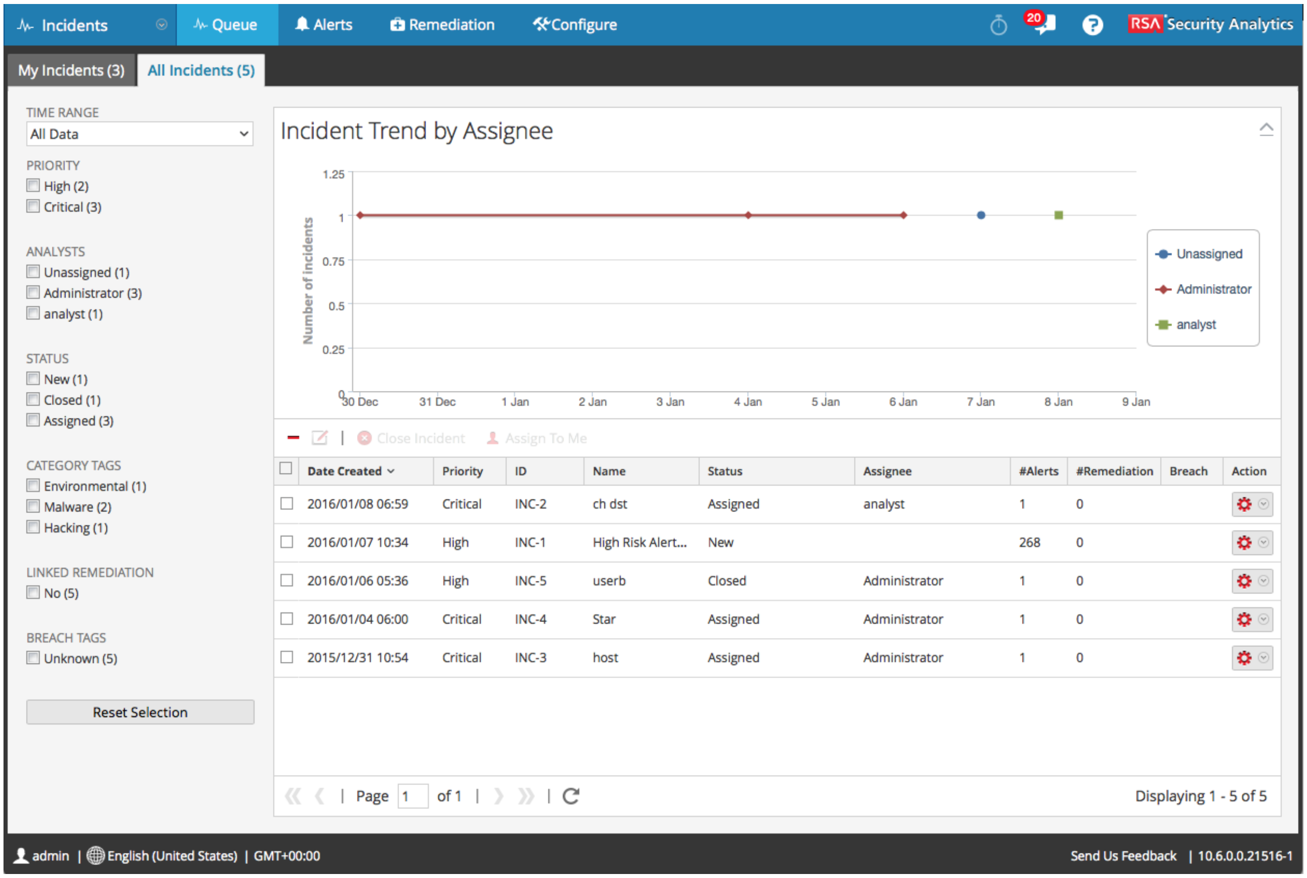
Features

This view has the following tabs:

- All Incidents - lists all incidents.
- My Incidents - lists all incidents assigned to you.

All Incidents Tab

This is an example of the All Incidents tab.



TIME RANGE
All Data

PRIORITY
□ High (2)
□ Critical (3)

ANALYSTS
□ Unassigned (1)
□ Administrator (3)
□ analyst (1)

STATUS
□ New (1)
□ Closed (1)
□ Assigned (3)

CATEGORY TAGS
□ Environmental (1)
□ Malware (2)
□ Hacking (1)

LINKED REMEDIATION
□ No (5)

BREACH TAGS
□ Unknown (5)

□	Date Created	Priority	ID	Name	Status	Assignee	#Alerts	#Remediation	Breach	Action
□	2016/01/08 06:59	Critical	INC-2	ch dst	Assigned	analyst	1	0		
□	2016/01/07 10:34	High	INC-1	High Risk Alert...	New		268	0		
□	2016/01/06 05:36	High	INC-5	userb	Closed	Administrator	1	0		
□	2016/01/04 06:00	Critical	INC-4	Star	Assigned	Administrator	1	0		
□	2015/12/31 10:54	Critical	INC-3	host	Assigned	Administrator	1	0		

Page 1 of 1

Displaying 1 - 5 of 5

The options panel has parameters that can be used to filter incidents. The filter parameters you choose to filter the incident queue are persisted and retained when you navigate away from the present view to switch between tabs, sessions or when you navigate to the incident details screen. The **Reset Selection** option enables you to reset the filter options to the default value.

Parameter	Description
TIME RANGE	Select a time range to view incidents in that time range. For example: • Select Last 24 Hours to view incidents created in the last 24 hours. • Select All Data to view all the incidents created. • Select Custom and provide a date range to view incidents created in that time frame.
PRIORITY	Indicates the number of incidents depending on their priorities. For example: Critical (18) indicates there are 18 incidents having priority set to Critical. Selecting one of the displayed options filters the incidents and displays only the incident priority selected. For example: If I select Critical (18), the Incident panel displays only the 18 incidents with a priority set to Critical.
ANALYSTS	This indicates the incidents categorized depending on to whom it is assigned.

Parameter	Description
STATUS	Indicates the incidents categorized depending on their status. For example: Assigned (7) indicates there are 7 incidents that are in the Assigned state. Selecting one of the displayed options filters the incidents and displays only the incidents belonging to the selected category. For example: If you select Assigned (7), the Incident panel displays only the 7 incidents that are in the Assigned state.
CATEGORY TAGS	Indicates the number of incidents belonging to a particular category. Since Categories are hierarchical, the category tags just count the parent category. For example: Malware (5) indicates there are 5 incidents belonging to the Malware category. Selecting one of the displayed options filters the incidents and displays only the incidents belonging to the selected category. For example: If I select Malware (5), the Incident panel displays only the 5 incidents that belong to the malware category.

Parameter	Description
LINKED REMEDIATION	Indicates the incidents categorized depending on whether they have remediation tasks or not. For example: Yes (5) indicates there are 5 incidents that have remediation tasks. No (3) indicates there are 3 incidents that have no remediation tasks. Selecting one of the displayed options filters the incidents and displays only the incidents depending on what is chosen. For example: If I select Yes (5), the Incident panel displays only the 5 incidents that have remediation tasks.
BREACH TAGS	Displays the breach tag associated with the incident.
Reset Selection	Resets filter options to default values.

The Incident hand panel has the following information:

On the top is a graphical representation of the incident trend by assignee and is one line per assignee. The graphical representation is based on the filter chosen. You can highlight the required line per assignee by disabling the other two in the box on the Incident side of the graph.

The lower part has a list of incidents and their details displayed as per the filter chosen.

Parameter	Description
Date Created	Displays the date when the incident was created.
Priority	Displays the priority of the incident. The priority can be any of the following: Critical, High, Medium, or Low.
ID	Displays the incident ID.
Name	Displays the incident name.
Status	Displays the work flow status of the incident.

Parameter	Description
Assignee	Displays the user to whom the incident is assigned to. This is visible only in the ALL Incidents details view.
#Alerts	Displays the number of alerts the incident is made up of.
#Remediation	Displays the number of remediation tasks created for the incident.
Breach	Displays whether the incident has a data breach, and if does it displays the breach tag.
Actions	Displays the actions that can be performed on the incident. The possible actions are: Assign to me, Edit Incident, and Close Incident.

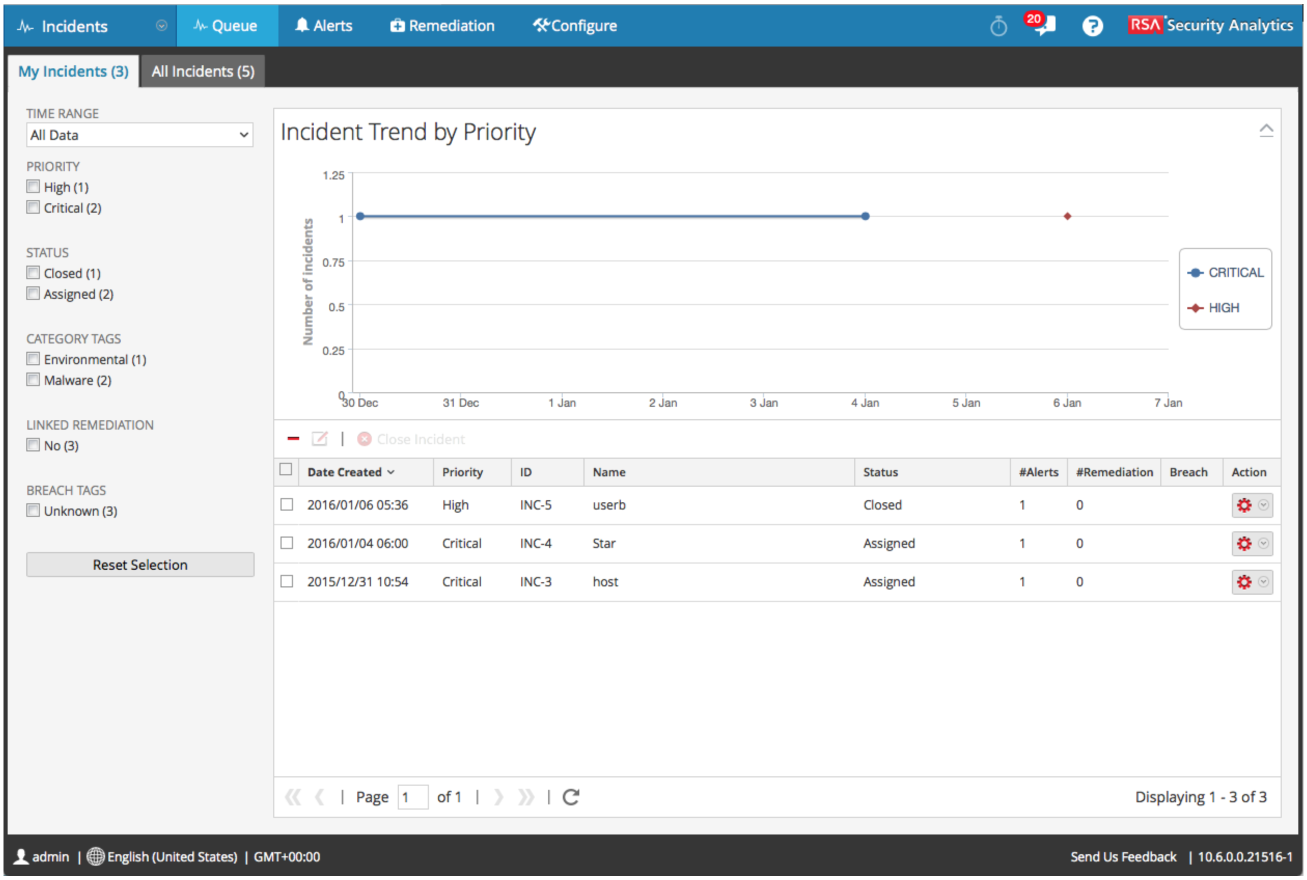
Operations

This table lists the operations that can be performed in the Summary view.

Parameter	Description
Assign to Me	Allows you to assign the incident to yourself. This option is available in the All Incidents view.
Edit Incident	Allows you to modify an incident.
Close Incident	Allows you to close an incident.
Delete	Allows you to delete an incident.
Report a Data Breach	Allows you report if there is a data breach. This is visible only if you have configured data breach support in the Integration Settings.

My Incidents Tab

This tab is visible only when there are incidents assigned to you. This figure is an example of the My Incidents tab.



TIME RANGE
All Data

PRIORITY
□ High (1)
□ Critical (2)

STATUS
□ Closed (1)
□ Assigned (2)

CATEGORY TAGS
□ Environmental (1)
□ Malware (2)

LINKED REMEDIATION
□ No (3)

BREACH TAGS
□ Unknown (3)

□	Date Created	Priority	ID	Name	Status	#Alerts	#Remediation	Breach	Action
□	2016/01/06 05:36	High	INC-5	userb	Closed	1	0		
□	2016/01/04 06:00	Critical	INC-4	Star	Assigned	1	0		
□	2015/12/31 10:54	Critical	INC-3	host	Assigned	1	0		

The options panel has parameters that can be used to filter incidents. The filter parameters you choose to filter the incident queue are persisted and retained when you navigate away from the present view to switch between tabs, sessions, or when you navigate to the incident details screen. The **Reset Selection** option enables you to reset the filter options to the default value.

Parameter	Description
TIME RANGE	Select a time range to view incidents in that time range. For example: • Select Last 24 Hours to view incidents created in the last 24 hours. • Select All Data to view all the incidents created. • Select Custom and provide a date range to view incidents created in that time frame.

Parameter	Description
PRIORITY	Indicates the number of incidents depending on their priorities. For example: Critical (18) indicates there are 18 incidents having priority set to Critical. Selecting one of the displayed options filters the incidents and displays only the incident priority selected. For example: If I select Critical (18), the Incident panel displays only the 18 incidents with a priority set to Critical.
STATUS	Indicates the incidents categorized depending on their status. For example: Assigned (2) indicates there are 2 incidents that are in the Assigned state. Selecting one of the displayed options filters the incidents and displays only the incidents belonging to the selected category. For example: If I select Assigned (2), the Incident panel displays only the 2 incidents that are in the Assigned state.
CATEGORY TAGS	Indicates the number of incidents belonging to a particular category. For example: Malware (5) indicates there are 5 incidents belonging to the Malware category. Selecting one of the displayed options filters the incidents and displays only the incidents belonging to the selected category. For example: If I select Malware (5), the Incident panel displays only the 5 incidents that belong to the malware category.

Parameter	Description
LINKED REMEDIATION	Indicates the incidents categorized depending on whether they have remediation tasks or not. For example: Yes (5) indicates there are 5 incidents that have remediation tasks. No (3) indicates there are 3 incidents that have no remediation tasks. Selecting one of the displayed options filters the incidents and displays only the incidents depending on what is chosen. For example: If I select Yes (5), the Incident panel displays only the 5 incidents that have remediation tasks.
BREACH TAGS	Displays the breach tag associated with the incident.
	Select this to reset the filter options to the default value.

On the top of the Incident panel is a graphical representation of the incidents assigned to you. The graph displays a trend by priority and is one line per priority. The graphical representation is based on the filter chosen. You can highlight the required line per priority by disabling the other priority options in the box on the right hand side of the graph.

The lower part has a list of incidents assigned to you and their details displayed as per the filter chosen.

You can accomplish the following operations from the My Incidents view:

- Edit an Incident
- Close an Incident
- Delete an incident
- Report a Data Breach

Incident Queue Details View

In the Incident Queue Details view, you can see details of an incident or edit an incident.

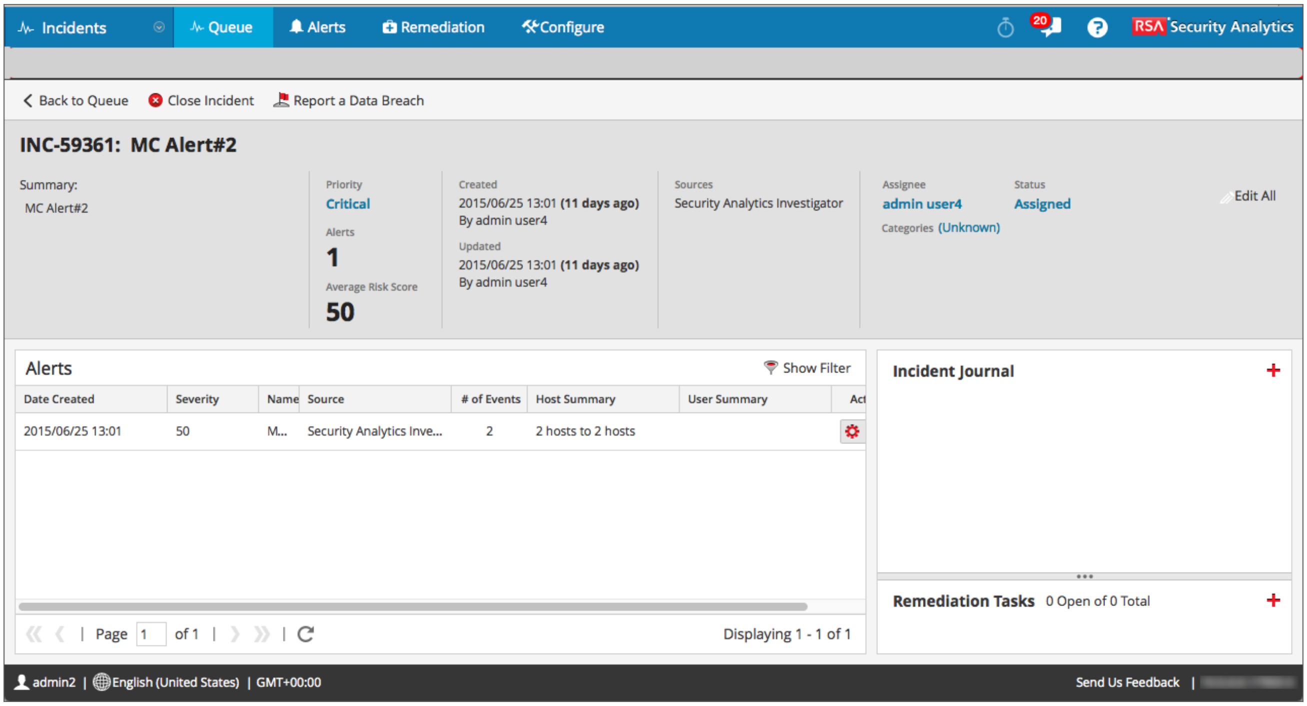
To access the Incident Queue Details view:

1. In the **Security Analytics** menu, select **Incidents** > **Queue**.

   The Incidents view is displayed.

2. Double-click one of the incidents.

   The Incidents Queue details view is displayed.



INC-59361: MC Alert#2

Summary: MC Alert#2

Priority: Critical

Alerts: 1

Average Risk Score: 50

Created: 2015/06/25 13:01 (11 days ago) By admin user4

Updated: 2015/06/25 13:01 (11 days ago) By admin user4

Sources: Security Analytics Investigator

Assignee: admin user4

Status: Assigned

Categories (Unknown)

Alerts

Date Created	Severity	Name	Source	# of Events	Host Summary	User Summary	Act
2015/06/25 13:01	50	M...	Security Analytics Inve...	2	2 hosts to 2 hosts		

Page 1 of 1 | Displaying 1 - 1 of 1

Remediation Tasks 0 Open of 0 Total

admin2 | English (United States) | GMT+00:00

Related procedures are available in View Incident Details.

Features

The following table lists the parameters displayed in the Incident Queue Details view.

Parameter	Description
Summary	Provides overall details for the risk alert.
Priority	Displays the priority of the task. This is an editable field.
Alerts	Displays the number of alerts.

Parameter	Description
Average Risk Score	Displays the average risk.
Created	Displays details about the date and time when the task was created and by whom it was created.
Updated	Displays the date and time when the task was last updated.
Sources	Displays where the incident came from.
Assignee	Displays the user to whom the incident is assigned to. This is an editable field.
Categories	Lists assigned categories.
Status	Displays the status of the incident. This is an editable field.

Toolbar

The following table lists the operations that can be performed in the Incident Queue Details view.

Parameter	Action
Back to Queue	Allows you to navigate back to Incident Queue view.
Close Incident	Allows you to close the current incident you are viewing.
Report a Data Breach	Sends a report of a data breach.
Edit All	Allows you to modify the incident as required.
Investigate Events	Allows you to closely investigate an event.
Investigate Source IP Address	Allows you to closely investigate IP Address of the Source.
Investigate Destination IP Address	Allows you to closely investigate IP Address of the Destination.
New Journal Entry	Allows you to create and publish a new journal entry.

Parameter	Action
New Remediation Task	Allows you to create a new remediation task.

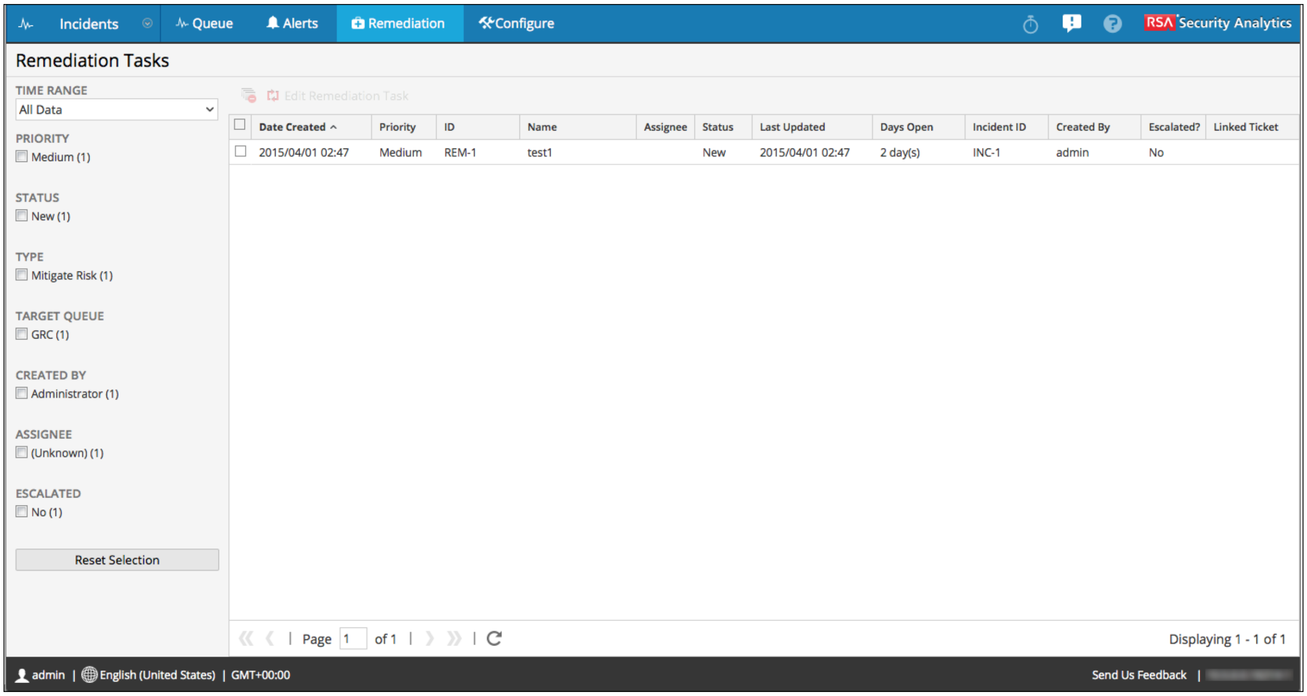
Remediation View

In the Remediation view, you can manage and track the remediation tasks, and do the following:

- Send a remediation task as a Helpdesk ticket where it can be managed in a third party helpdesk system and tracked to closure.
- Send a remediation task to RSA Archer so that it is tracked by the RSA Security Operations Management solution.

These two options are available if these integration settings are configured in the Integration Settings.

To access the Remediation Tasks view, in the **Security Analytics** menu, select **Incidents** > **Remediation**. The Remediation Tasks view is displayed. It is a list of all remediation tasks.



Remediation Tasks

TIME RANGE
All Data

PRIORITY
□ Medium (1)

STATUS
□ New (1)

TYPE
□ Mitigate Risk (1)

TARGET QUEUE
□ GRC (1)

CREATED BY
□ Administrator (1)

ASSIGNEE
□ (Unknown) (1)

ESCALATED
□ No (1)

□	Date Created ^	Priority	ID	Name	Assignee	Status	Last Updated	Days Open	Incident ID	Created By	Escalated?	Linked Ticket
□	2015/04/01 02:47	Medium	REM-1	test1		New	2015/04/01 02:47	2 day(s)	INC-1	admin	No	

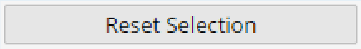
Features

The Remediation Tasks view consists of two panels and a toolbar.

The options panel, on the left, has parameters that can be used to filter the remediation tasks.

Parameter	Description
TIME RANGE	Select a time range to view remediation tasks created in the selected time range. For example: • Select **Last 24 Hours** to view remediation tasks created in the last 24 hours. • Select **All Data** to view remediation tasks created from the time the host was installed. • Select **Custom** and provide a date range to view remediation tasks created in that time frame.
PRIORITY	Indicates the number of remediation tasks depending on their priorities. For example: Critical (2) indicates there are 2 remediation tasks having priority set to Critical. Selecting one of the displayed options filters the remediation tasks and displays only the remediation tasks of the priority selected. For example: If you select Critical (2), the Remediation Tasks panel displays only the 2 remediation tasks with a priority set to Critical.
STATUS	Indicates the number of remediation tasks belonging to a particular status. For example: Assigned (5) indicates there are 5 remediation tasks in the Assigned state. Selecting one of the displayed options filters the remediation tasks and displays only the tasks belonging to the selected status. For example: If you select Assigned (5), the Remediation Tasks panel displays only the 5 tasks that belong to the Assigned state.

Parameter	Description
TYPE	Indicates the number of remediation tasks categorized by their type. For example: Quarantine host (2) indicates there are 2 tasks of the type Quarantine host. Selecting one of the displayed options filters the tasks and displays only the tasks of the selected type. For example: If you select Quarantine host (2), the Remediation Tasks panel displays only the 2 incidents that are of the type Quarantine host.
TARGET QUEUE	Indicates the remediation tasks categorized depending on the Assignment queue. For example: Operations (5) indicates there are 5 incidents that have remediation tasks with the assignment queue for Operations. Selecting one of the displayed options filters the tasks and displays only the tasks depending on what is chosen. For example: If you select Operations (5), the Remediation Tasks panel displays only the 5 tasks that are in the assignment queue for Operations.
CREATED BY	Indicates the remediation tasks categorized depending on who created the tasks. For example: Admin (3) indicates there are 3 remediation tasks created by the Admin. Selecting one of the displayed options filters the tasks and displays only the tasks depending on what is chosen. For example: If you select Admin (3), the Remediation Tasks panel displays only the 3 tasks that are created by the Admin.

Parameter	Description
ASSIGNEE	Indicates the remediation tasks categorized depending on who it is assigned to. For example: <user1> (3) indicates there are 3 remediation tasks assigned to user1. Selecting one of the displayed options filters the tasks and displays only the tasks depending on what is chosen. For example: If you select <user1> (3), the Remediation Tasks panel displays only the 3 tasks that are assigned to user1.
ESCALATED	Indicates the remediation tasks that are escalated.
	Resets filter options to default values

The Remediation Tasks panel has a list of remediation tasks and their details.

Parameter	Description
Date Created	Displays the date when the remediation task was created.
Priority	Displays the priority assigned to the remediation task. The priority can be any of the following: Critical, High, Medium, or Low.
ID	Displays the remediation task ID.
Name	Displays the remediation task name.
Assignee	Displays the name of the user to whom the remediation task is assigned to.
Status	Displays the status of the remediation task. For example, New, In Progress, Remediated.
Last Updated	Displays the date and time when the remediation task was last updated.
Days Open	Displays the number of days the remediation task has been open.

Parameter	Description
Incident ID	Displays the Incident ID of the incident to which the remediation task is created for.
Created By	Displays the user who created the remediation task.
Escalated?	Displays whether the remediation task has been escalated.
Linked Ticket	Displays the whether the remediation task was sent as a help desk ticket or to any other third party solution.

Toolbar

This table lists the operations that can be performed in the Remediation Tasks view.

Parameter	Description
⊖	Allows you to delete remediation task(s).
Edit Remediation Task	Allows you to modify the remediation task.
Send to Help Desk	Allows you to send the remediation task to Help Desk.
Send to RSA Archer	Allows you to send the remediation task to RSA Archer.

Remediation Task Details View

In the Remediation Task details view you can see the details of the remediation task, modify the remediation task, and view the details of the incident for which it was created.

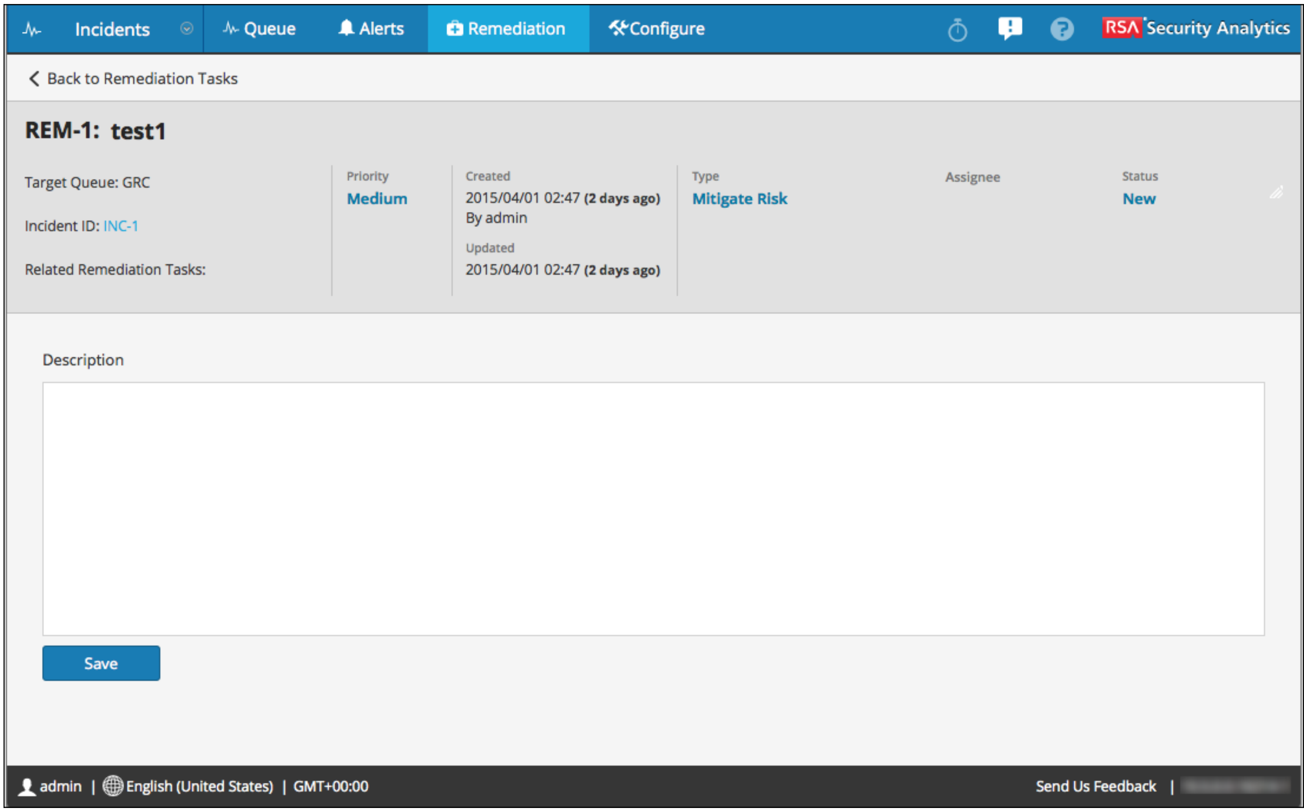
To access the Remediation Task details view:

1. In the **Security Analytics** menu, select **Incidents** > **Remediation**.

   The Remediation tasks view is displayed.

2. Double-click one of the remediation tasks.

   The Remediation Task details view is displayed.



REM-1: test1

Target Queue: GRC

Incident ID: INC-1

Related Remediation Tasks:

Priority: Medium

Created: 2015/04/01 02:47 (2 days ago) By admin

Updated: 2015/04/01 02:47 (2 days ago)

Type: Mitigate Risk

Assignee

Status: New

Description

Features

The following table lists the parameters displayed in the Remediation Task details view.

Parameter	Description
Target Queue	Displays the target queue to which the task is assigned.

Parameter	Description
Incident ID	Displays the Incident ID for which the task was created. Click the ID to display the details of the Incident.
Related Remediation Tasks	Displays the related remediation tasks. Click the related task to navigate to the related task view.
Priority	Displays the priority of the task. This is an editable field.
Created	Displays details about the date and time when the task was created and by whom was it created.
Updated	Displays the date and time when the task was last updated.
Type	Displays the type by which the remediation task is categorized. This is an editable field.
Assignee	Displays the user to whom the remediation task is assigned to. This is an editable field.
Status	Displays the status of the remediation task. This is an editable field.

Toolbar

This table lists the operations that can be performed in the Remediation Task details view.

Parameter	Action
Back to Remediation Tasks	Allows you to navigate back to the Remediation Tasks view.
Send to Help Desk	Allows you to push the task to the Helpdesk. This option is visible only when it is configured in integration settings.
Send to RSA Archer	Allows you to send the task to RSA Archer Solution. This option is visible only when it is configured in integration settings.

Parameter	Action
Edit	Allows you to modify the task as required. You can modify the following parameters: Type, Priority, Assignee, and Status.