



RSA | Security Analytics

Incident Management Configuration 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

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

License Agreement

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

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

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

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

May 2018

Contents

Incident Management Configuration Guide Overview	4
Incident Management Overview	5
Configure Incident Management	7
Step 1. Add Incident Management Service	8
Prerequisites	8
Procedure	8
Step 2. Configure a Database for the Incident Management Service	10
Considerations for Choosing the Host for ESA Database	10
Prerequisites	10
Procedure	11
Step 3. Configure Alert Sources to Display Alerts in Incident Management	12
Prerequisites	12
Configure Reporting Engine to Display Alerts Triggered by Reporting Engine in Incident Management View	12
Configure Malware Analytics to View Alerts Triggered by Malware Analytics in Incident Management view	13
Configure ECAT to View Alerts Triggered by ECAT in Incident Management View	13
Configure ECAT to Display ECAT Alerts	14
Set Counter for Matched Alerts and Incidents	16
Incident Management Services System View	18
Access the View	18
Service Information	18

Incident Management Configuration Guide

Overview

This guide provides an overview of Incident Management, detailed instructions on how to configure Incident Management in your network, additional procedures that are used at other times, and reference materials that describe the user interface for configuring Incident Management in your network.

Topics

- [Incident Management Overview](#)
- [Configure Incident Management](#)
- [Set Counter for Matched Alerts and Incidents](#)
- [Incident Management Services System View](#)

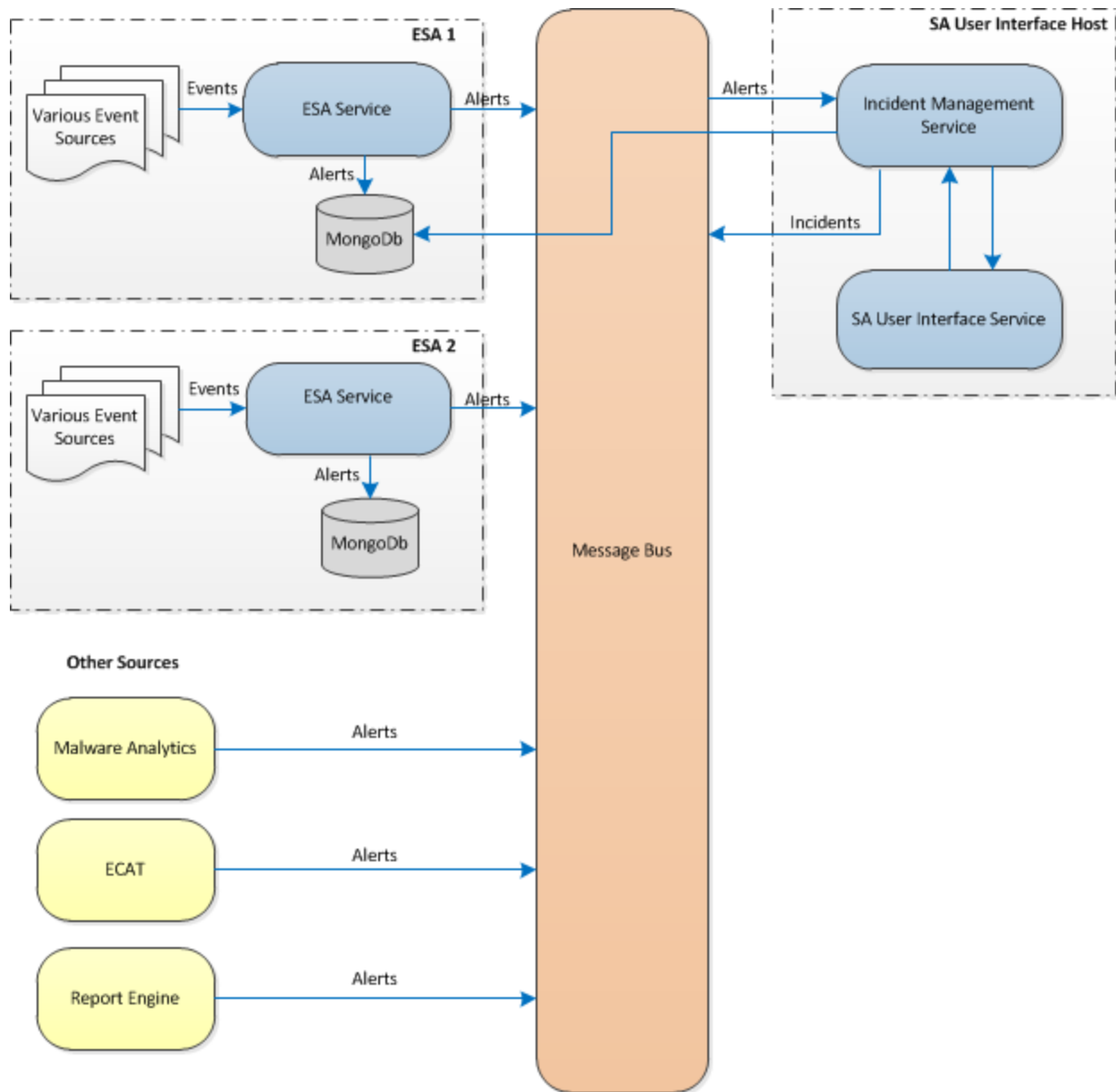
Incident Management Overview

Security Analytics Incident Management consumes Alert data from various sources via the Message Bus and displays these alerts on the Security Analytics User Interface. The Incident Management service allows you to group the alerts logically and start an Incident response workflow to investigate and remediate the security issues raised.

The Incident Management service consumes alerts from the message bus and normalizes the data to a common format (while retaining the original data) to enable simpler rule processing. It periodically runs rules to aggregate multiple alerts into an incident and set some attributes of the Incident (for example, severity, category, and so on). The incidents are persisted into MongoDB by the Incident Management service. Incidents are also posted onto the message bus for consumption by other systems (for example, Archer integration).

Note: Alert records are persisted in MongoDB by the Incident Management service. In Security Analytics 10.4 and above, the instance of MongoDB is installed on one of the ESA hosts. ESA is a required component for Incident Management.

The following figure illustrates a high level data flow diagram:



You have to configure various sources from which the alerts are collected and aggregated by the Incident Management service.

Configure Incident Management

This topic provides the high-level tasks required to configure the Incident Management service. The administrator needs to complete the steps in the sequence provided.

Topics

- [Step 1. Add Incident Management Service](#)
- [Step 2. Configure a Database for the Incident Management Service](#)
- [Step 3. Configure Alert Sources to Display Alerts in Incident Management](#)

Step 1. Add Incident Management Service

This topic provides information on how to add the Incident Management service on a host.

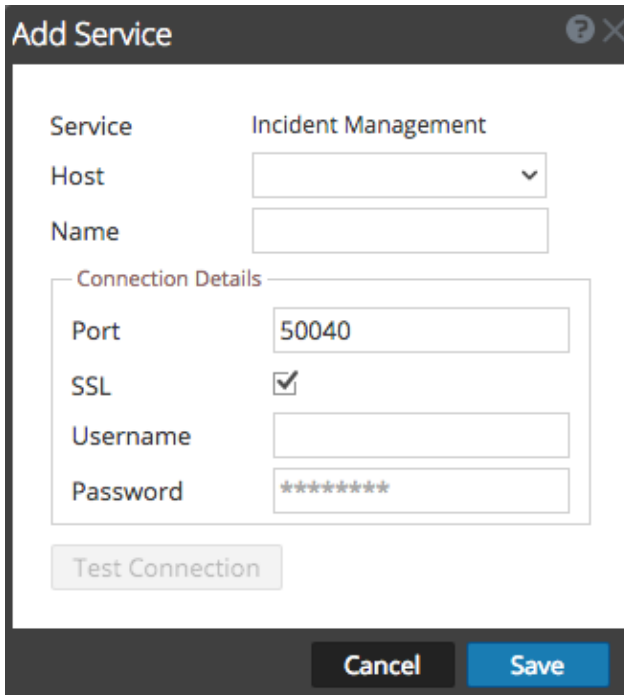
Prerequisites

Ensure that you have installed a host on which you want to run the Incident Management service. Refer to **Step 1: Add or Update a Host** in the *Hosts and Services Getting Started Guide* for the procedure to add a host.

Procedure

To add the Incident Management service:

1. In the **Security Analytics** menu, select **Administration > Services**.
The services view is displayed.
2. In the Services panel, select **+** > **Incident Management**.
The **Add Service** dialog is displayed.



The screenshot shows the 'Add Service' dialog box with the following fields and options:

- Service:** Incident Management
- Host:** A dropdown menu.
- Name:** A text input field.
- Connection Details:**
 - Port:** 50040
 - SSL:**
 - Username:** A text input field.
 - Password:** A text input field with masked characters (*****).
- Test Connection:** A button.
- Cancel:** A button.
- Save:** A button.

3. Provide the following details:

Field	Description
Host	Select the host on which the IM server is installed.
Name	Type a name for the service.
Port	Default port is 50040.
SSL	Select SSL if you want Security Analytics to communicate with the host using SSL. The security of data transmission is managed by encrypting information and providing authentication with SSL certificates. This is required by default. <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Note: If you select SSL, ensure SSL is enabled in the System Configuration panel.</p> </div>
Username	Type the username of the host.
Password	Type the password of the host.

4. Click **Test Connection** to determine if Security Analytics connects to the service.
5. When the result is successful, click **Save**.

The added service is now displayed in the services panel.

Note: If the test is unsuccessful, edit the service information and retry.

Step 2. Configure a Database for the Incident Management Service

You have to configure the database for the Incident Management service for it to become usable. The ESA installation creates and secures a database instance for Incident Management service. You have to select one of the ESA servers to act as the database host for the Incident Management Service.

Considerations for Choosing the Host for ESA Database

This topic applies if you enable cross-site correlation in ESA.

In ESA, cross-site correlation allows you to create a deployment that includes one set of rules and multiple ESA services. These are the main features of a cross-site correlation deployment:

1. There is one central ESA service.
2. When you deploy rules, ESA services forward relevant events to the central ESA.
3. The central ESA runs the rules and generates alerts.

If you enable cross-site correlation, there are factors to consider when you choose which ESA to use with Incident Management:

- Choose an ESA service that is co-located with Security Analytics to limit latency for access to MongoDB.
- Choose the ESA that gets the least traffic.

Note: Do not choose the central ESA because it ingests its own traffic and receives forwarded events from other ESA services.


By default, cross-site correlation is not enabled. To enable cross-site correlation, you must consult with RSA Professional Services to take part in the Cross-Site Correlation Field Trial Program.

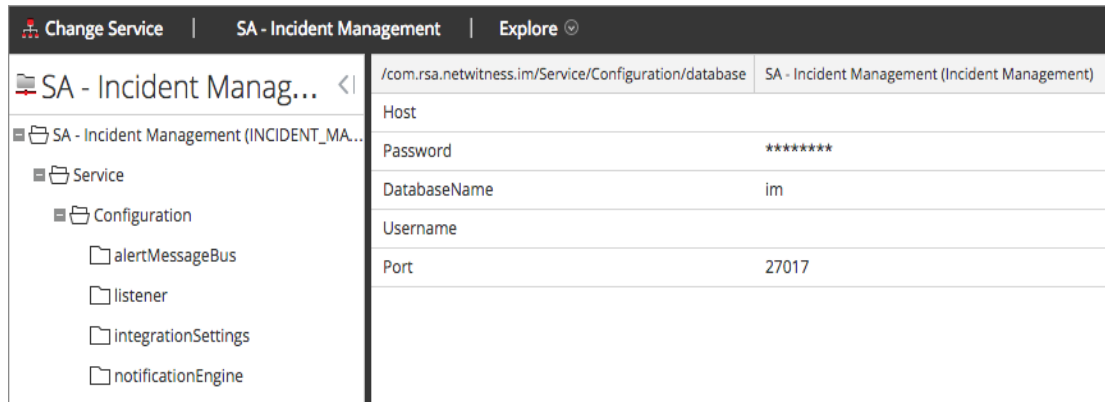
Prerequisites

Ensure that an ESA host is installed and configured.

Procedure

To configure a database for the Incident Management service:

1. In the **Security Analytics** menu, select **Administration > Services**.
The Services view is displayed.
2. In the Services panel, select the Incident Management Service, and  > **View > Explore**.
The Services Explore view is displayed.
3. In the options panel, select **Service > Configuration > database**.
The database view is displayed in the right side panel.



4. Provide the following information:
 - **Host** – The hostname or IP address of the ESA host selected as a database
 - **DatabaseName** – im (this is the default value)
 - **Port** – 27017 (this is the default value)
 - **Username** – The username for the user account for the IM database (ESA creates an im user with the right privileges)
 - **Password** – The password you selected for the im user
5. Restart the Incident Management service using the following command.

```
service rsa-im restart
```

Note: Restarting the Incident Management service is important for the database configuration to be complete.

Step 3. Configure Alert Sources to Display Alerts in Incident Management

This procedure is required so that alerts from the alert sources are displayed in Incident Management. You have an option to enable or disable the alerts being populated in the Incident Management view. By default this option is disabled in the Reporting Engine, Malware Analytics, and ECAT and enabled only in Event Stream Analysis. So when you install the Incident Management service you need to enable this option in the Reporting Engine, Malware Analytics, and ECAT to populate the corresponding alerts in the Incident Management view.


Prerequisites

Ensure that:

- The Incident Management service is installed and running on Security Analytics.
- A database is configured for the incident management service.
- ECAT is installed and running.

Configure Reporting Engine to Display Alerts Triggered by Reporting Engine in Incident Management View

The Reporting Engine alerts are by default disabled from being displayed in Incident Management view. To display and view the Reporting Engine alerts, you have to enable the Incident Management alerts in the Services Config view > General tab for the Reporting Engine.

1. In the **Security Analytics** menu, select **Administration > Services**.
2. Select a Reporting Engine service, and select  > **View > Config**.
The Services Config view is displayed with the Reporting Engine General tab open.
3. Select **System Configuration**.
4. Select the checkbox for **Forward Alerts to IM**.
The Reporting Engine now forwards the alerts to Incident Management.

For details on parameters in the General tab, see the **Reporting Engine General Tab** topic in the *Reporting Engine Configuration Guide*.

Configure Malware Analytics to View Alerts Triggered by Malware Analytics in Incident Management view

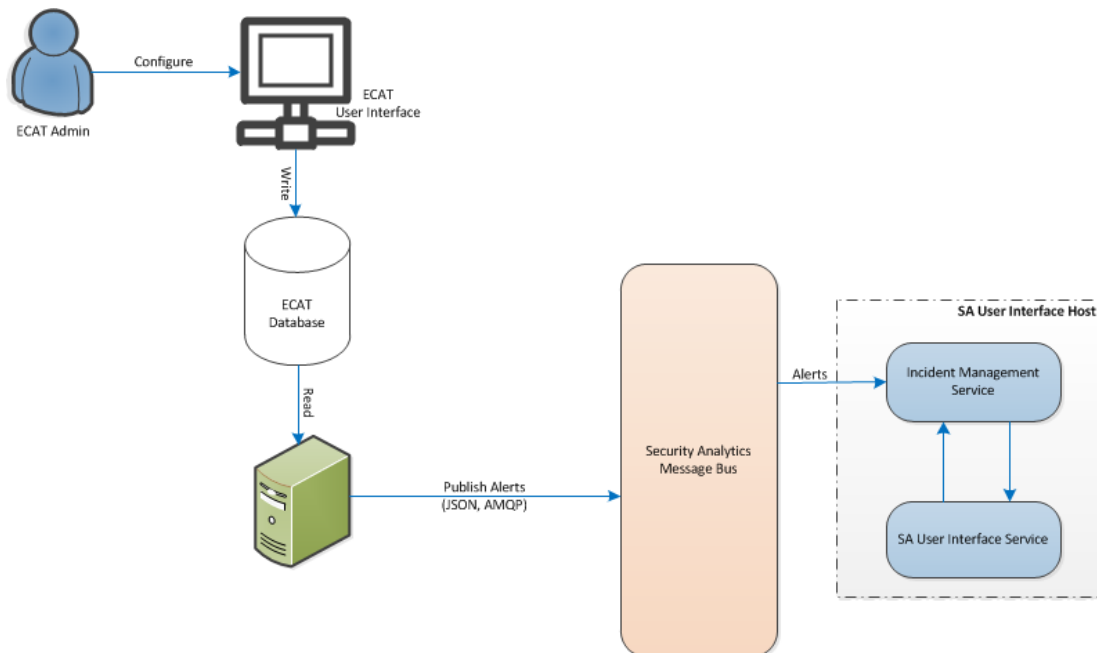
Viewing Incident Management alerts is a function of auditing in Malware Analysis. The procedure of enabling IM alerts is described in the **(Optional) Configure Auditing on Malware Analysis Host** topic in the *Malware Analysis Configuration Guide*.

Configure ECAT to View Alerts Triggered by ECAT in Incident Management View

This procedure is required to integrate ECAT with Security Analytics so that the ECAT alerts are picked up by the Incident Management component of Security Analytics and displayed in the **Incident > Alerts** view.

Note: The **RSA ECAT Integration** topic in the *RSA ECAT Integration Guide* provides an overview of ECAT integration capabilities in Security Analytics as well as detailed procedures for configuring integration of ECAT with Security Analytics via the Message Bus.

The diagram below represents the flow of ECAT alerts to the Incident Management queue of Security Analytics and its display in the **Incident > Alerts** view.



Configure ECAT to Display ECAT Alerts

To configure ECAT to display ECAT alerts in the Security Analytics user interface:

1. In the ECAT User Interface, click **Configure > Monitoring and External Components**.
The **Monitoring and External Components** dialog is displayed.
2. Right-click anywhere on the dialog and select **Add Component**.
The **Add Component** dialog is displayed.
3. Provide the following information:
 - Select IM broker for the **Component Type** from the drop-down options.
 - Type a user name to identify the IM broker.
 - Type the **Host DNS or IP address** of the IM broker.
 - Type the **Port number**. The default port is 5671.
4. Click **Save and Close** to close all the dialogs.
5. To set up SSL for IM Alerts, perform the following steps on the ECAT to set the SSL communications:
 - a. On the ECAT primary console server, export the ECAT CA certificate to cer format (Base-64 encoded X.509) from the Local Computer's personal certificate store (without selecting the private key).
 - b. On ECAT primary console server, generate a client certificate for ECAT using the ECAT CA certificate. (The CN name MUST be set to ecat.)

```
makecert -pe -n "CN=ecat" -len 2048 -ss my -sr LocalMachine -a sha1 -sky exchange -eku 1.3.6.1.5.5.7.3.2 -in "EcatCA" -is MY -ir LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -cy end -sy 12 client.cer
```
 - c. On ECAT primary console server, make a note of the thumbprint of the client certificate generated in step b. Enter the thumbprint value of the client certificate in the `IMBrokerClientCertificateThumbprint` section of the `ConsoleServer.Exe.Config` file as shown.

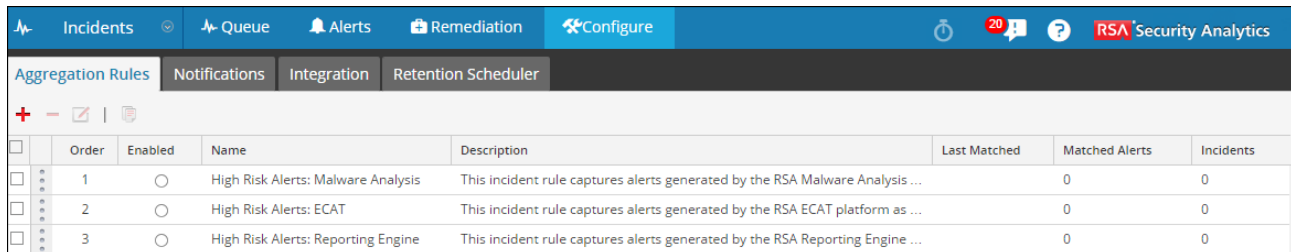
```
<add key="IMBrokerClientCertificateThumbprint" value="?896df0efacf0c976d955d5300ba0073383c83abc"/>
```
 - d. On the SA server, append the content of the ECAT CA certificate file in .cer format (from step a) to `/etc/puppet/modules/rabbitmq/files/truststore.pem`.
 - e. On the SA server, run puppet agent as shown (or wait 30 minutes for SA server to run).

```
puppet agent -t
```

- f. On ECAT primary console server, import the `/var/lib/puppet/ssl/certs/ca.pem` file from SA server to Trusted Root Certification Authorities store. This will ensure that the ECAT as a client, will be able to trust the IM server certificate

Set Counter for Matched Alerts and Incidents

This procedure is optional. Administrators can use it to change when the count for matched alerts is reset to 0. The Aggregation Rules tab displays these counts in columns on the right.



	Order	Enabled	Name	Description	Last Matched	Matched Alerts	Incidents
<input type="checkbox"/>	1	<input type="radio"/>	High Risk Alerts: Malware Analysis	This incident rule captures alerts generated by the RSA Malware Analysis ...		0	0
<input type="checkbox"/>	2	<input type="radio"/>	High Risk Alerts: ECAT	This incident rule captures alerts generated by the RSA ECAT platform as ...		0	0
<input type="checkbox"/>	3	<input type="radio"/>	High Risk Alerts: Reporting Engine	This incident rule captures alerts generated by the RSA Reporting Engine ...		0	0


These columns provide the following information for a rule:

- **Last Matched** column shows the time when the rule last matched alerts.
- **Matched Alerts** column displays the number of matched alerts for the rule.
- **Incidents column** displays the number of incidents created by the rule.

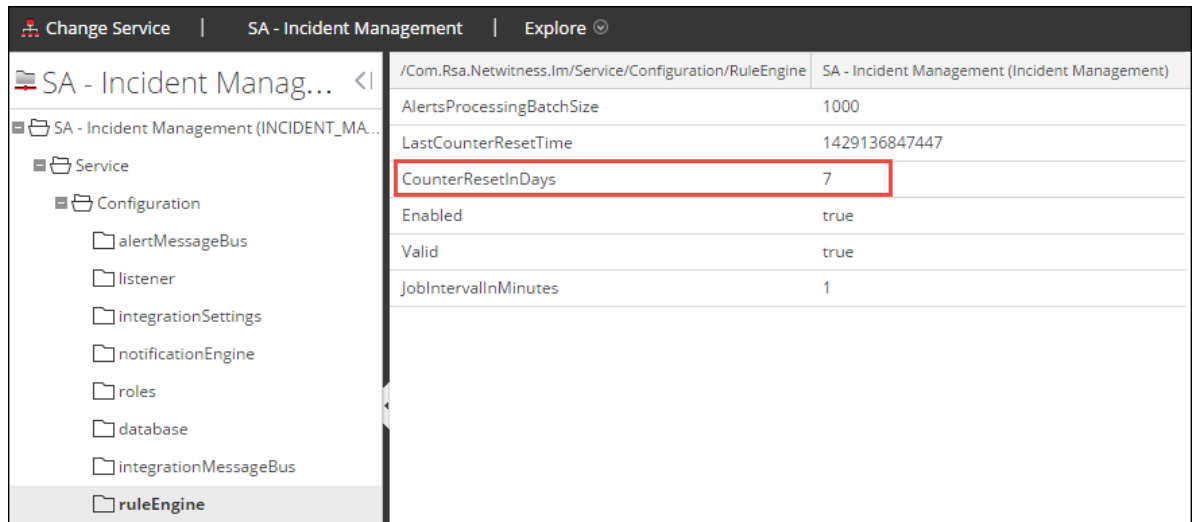
By default, these values reset to zero every 7 days. Depending on how long you want the counts to continue, you can change the default number of days.


Note: When the counter resets to zero, only the numbers in the three columns change to zero. No alerts or incidents get deleted.

To set a counter for matched alerts and incidents:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. Select an Incident Management service, then select  > **View > Explore**.

- In the Explore view on the left, select **Service > Configuration > ruleEngine**.




- In the right panel, type the number of days in the **CounterResetInDays** field.
- Restart the service for the new setting to take effect:
 - Select **Services**.
 - Select the service, then click  > **Restart**.

Incident Management Services System View

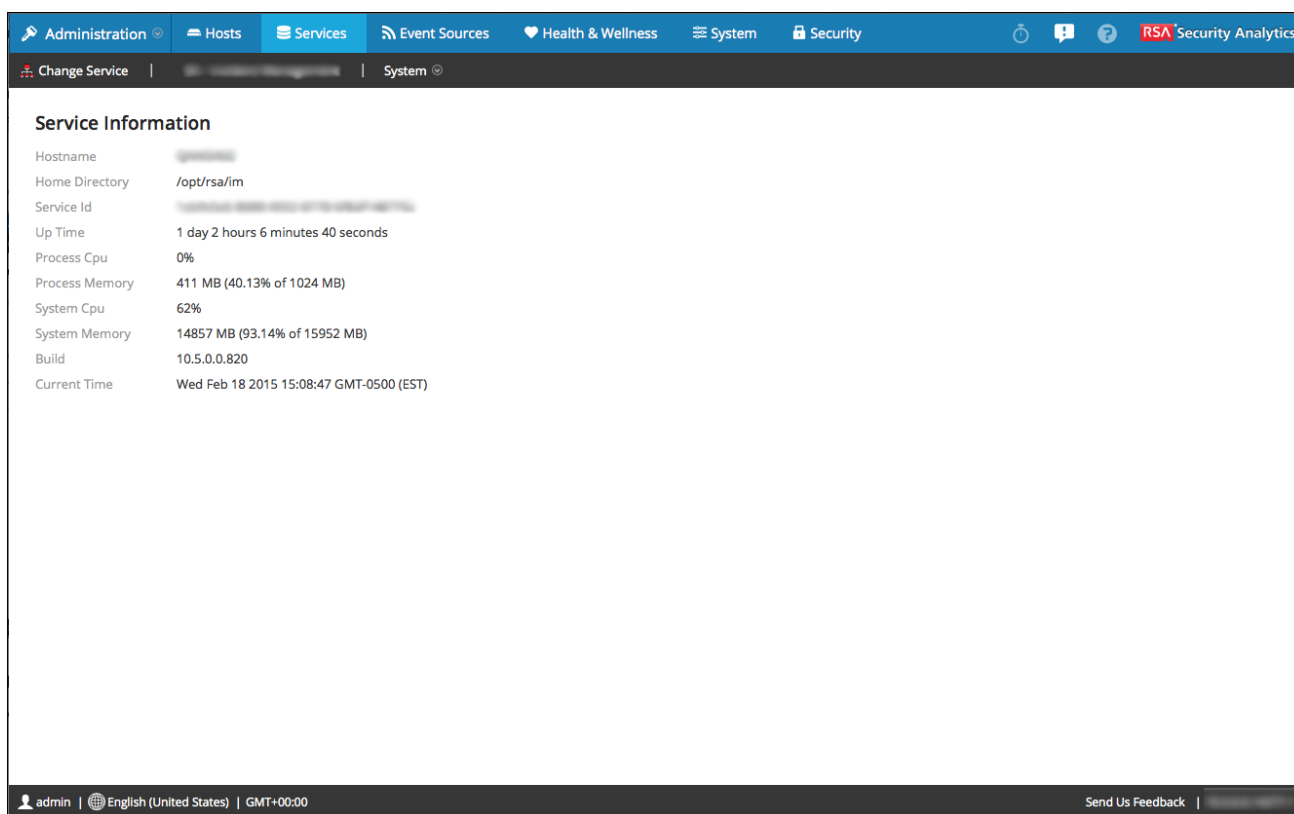
In the Services System view, you can view information about the Incident Management service.

Access the View

To access this view:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select an Incident Management service and  > **View > System**.

The Services System view for Incident Management is displayed.



Service Information

The System view contains one panel: the Service Information panel. The Service Information panel provides a service summary, which is slightly different than the generic Services System view. This table describes the service information in the panel.

Field	Description
Hostname	Displays the hostname. For example: NWAPPLIANCE2682
Home Directory	Displays the location of the Incident Management home directory. For example: /opt/rsa/im
Service Id	Displays the service ID. For example: 1694b15c-42c7-410d-9ba3-a7c48ba4722d
Up Time	Displays the amount of time that has passed since the host started. For example: 0 5 hours 33 minutes 20 seconds
Process Cpu	Displays the percentage of CPU used by the process. For example: 0%
Process Memory	Displays the memory used by the process. For example: 86285 KB (8.37% of 1024 MB)
System Cpu	Displays the percentage of CPU used by the system. For example: 2%
System Memory	Displays the memory used by the system. For example: 30065 MB (31.05% of 96831 MB)
Build	Displays the version number of Security Analytics. For example: 10.6.0.0.1009
Current Time	Displays the current day of the week, date, and time. For example: Thu Jan 14 2016 11:15:23 GMT-0500 (EST)

