



NetWitness Respond Configuration Guide

for RSA NetWitness® Platform 11.3



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at <https://community.rsa.com> contains a knowledge base 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 <https://www.rsa.com/en-us/company/rsa-trademarks>.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, 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 Dell.

Third-Party Licenses

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

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

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

July 2019

Contents

- About this Document 6**
- NetWitness Respond Configuration Overview 7**
- Configuring NetWitness Respond 9**
 - Step 1. Configure Alert Sources to Display Alerts in the Respond View 10
 - Prerequisites 10
 - Configure Reporting Engine to Display Reporting Engine Alerts in the Respond View 10
 - Configure Malware Analysis to Display Malware Analysis Alerts in the Respond View 11
 - Configure NetWitness Endpoint to Display NetWitness Endpoint Alerts in the Respond View ... 11
 - Step 2. Assign Respond View Permissions 14
 - Respond-server 15
 - Incidents 16
 - Integration-server 16
 - Investigate-server 16
 - Respond Notification Settings Permissions 17
 - Respond Event Analysis Permissions 17
 - Respond Role Permission Examples 18
 - Step 3. Enable and Create Incident Rules for Alerts 19
 - Enable an Incident Rule 19
 - Create an Incident Rule 21
 - Verify the Order of Your Incident Rules 23
 - Clone an Incident Rule 24
 - Edit an Incident Rule 24
- Additional Procedures for Respond Configuration 25**
 - Set Up and Verify Default Incident Rules 26
 - Set Up the User Behavior Incident Rule 26
 - Set up or Verify a Default Incident Rule 30
 - Create a NetWitness Endpoint Incident Rule using File Hash 39
 - Configure Risk Scoring Settings for Automated Incident Creation 41
 - Configure Respond Email Notification Settings 44
 - Set a Retention Period for Alerts and Incidents 46
 - Prerequisites 46
 - Procedure 46
 - Result 47
 - Set a Retention Period for Risk Scoring Data 48
 - Prerequisites 48

Procedure	48
Result	48
Obfuscate Private Data	49
Prerequisites	49
Procedure	49
Manage Incidents in Archer Cyber Incident & Breach Response	51
Prerequisites	51
Procedure	51
Configure the Option to Send Incidents to RSA Archer	53
Configure Threat Aware Authentication	55
Enable Threat Aware Authentication	55
Configure Sync Frequency	57
Set Counter for Matched Alerts and Incidents	58
Configure a Database for the Respond Server Service	60
Prerequisites	60
Procedure	60
NetWitness Respond Configuration Reference	62
Configure View	62
Incident Rules View	63
What do you want to do?	63
Related Topics	63
Quick Look	64
Endpoint Risk Scoring Settings	65
Incident Rules	67
Incident Rule Details View	69
What do you want to do?	69
Related Topics	69
Quick Look	69
Group By Meta Key Mappings	73
Respond Notification Settings View	75
What do you want to do?	75
Related Topics	75
Quick Look	75
Aggregation Rules Tab	78
What do you want to do?	78
Related Topics	78
Quick Look	78
New Rule Tab	80
What do you want to do?	80
Related Topics	80

Quick Look 80

About this Document

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

Topics

- [NetWitness Respond Configuration Overview](#)
- [Configuring NetWitness Respond](#)
- [Additional Procedures for Respond Configuration](#)
- [NetWitness Respond Configuration Reference](#)

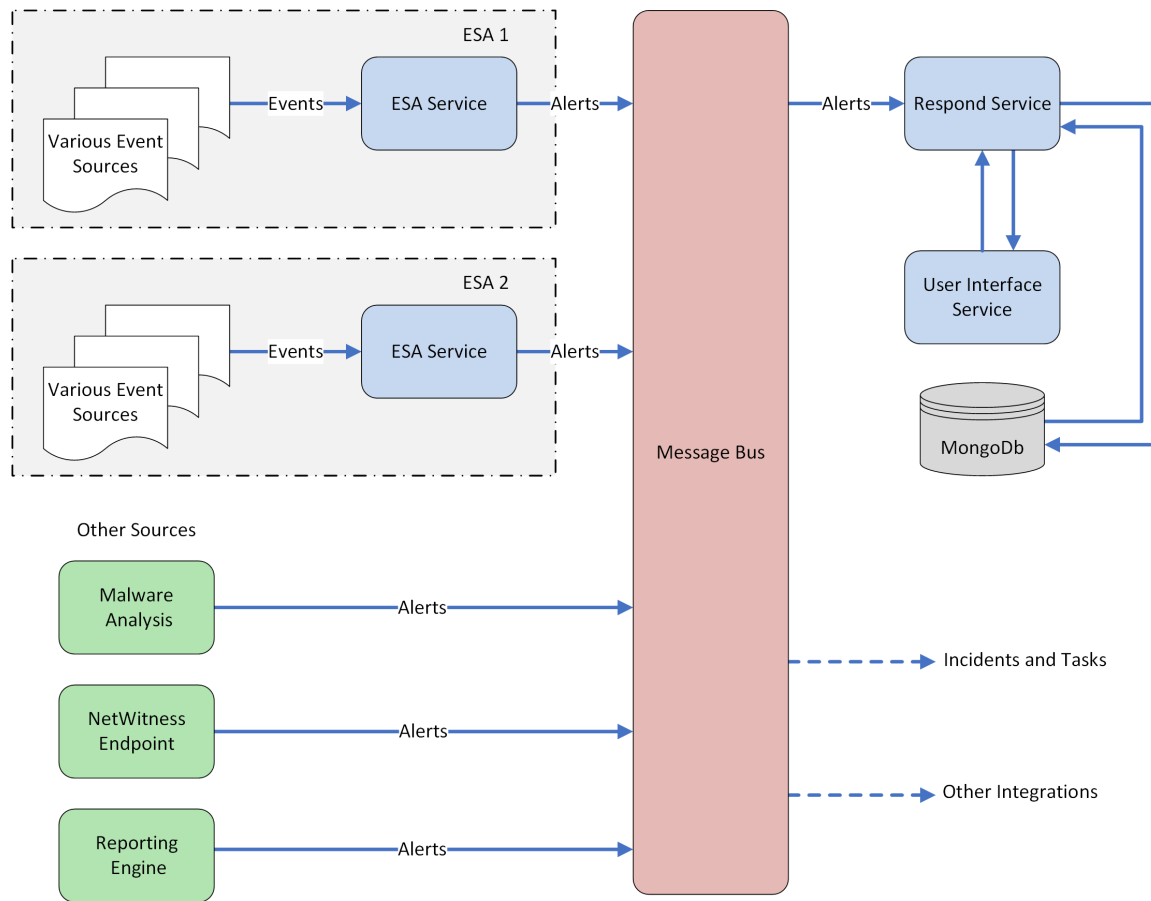
NetWitness Respond Configuration Overview

NetWitness Respond consumes alert data from various sources via the Message Bus and displays these alerts on the NetWitness Platform user interface. The Respond Server service allows you to group the alerts logically and start a NetWitness Respond workflow to investigate and remediate the security issues raised.

The Respond Server 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 Respond Server service. Incidents are also posted onto the message bus for consumption by other systems (for example, Archer integration).

Note: NetWitness Respond requires an ESA primary server that contains the MongoDB. Alerts, Incidents, and Task records are persisted into this MongoDB by the Respond Server.

The following diagram illustrates the high-level flow of alerts.



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

Configuring NetWitness Respond

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

Topics

- [Step 1. Configure Alert Sources to Display Alerts in the Respond View](#)
- [Step 2. Assign Respond View Permissions](#)
- [Step 3. Enable and Create Incident Rules for Alerts](#)

Step 1. Configure Alert Sources to Display Alerts in the Respond View

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



Prerequisites

Ensure that:

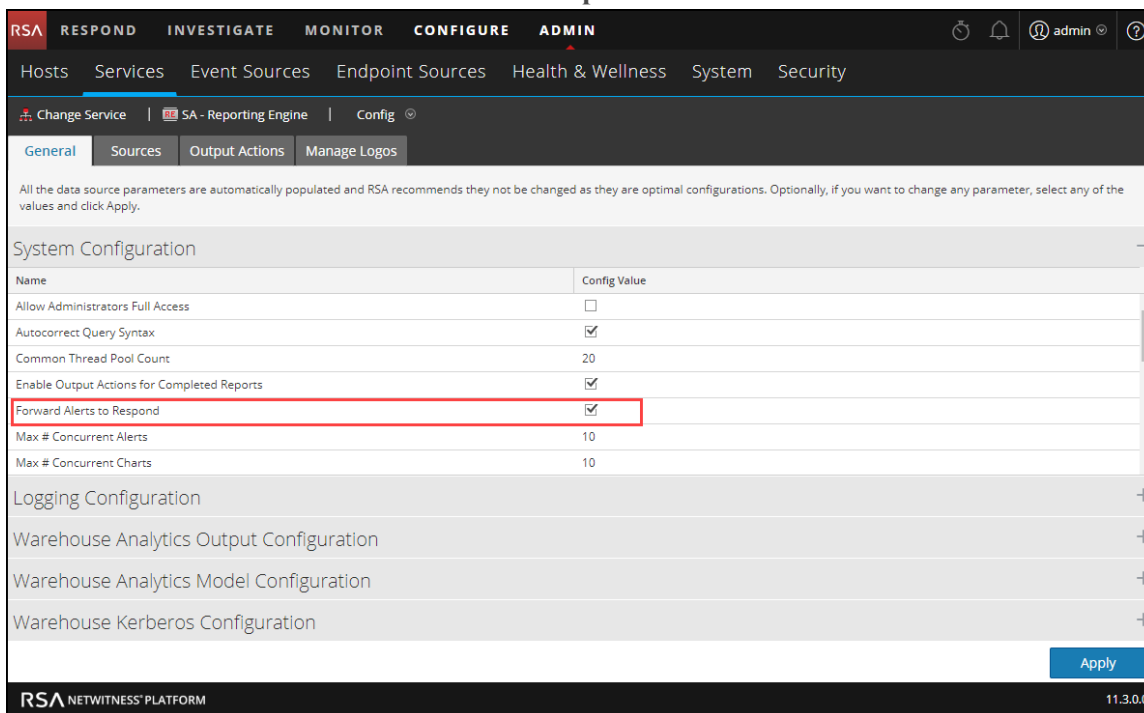
- The Respond Server service is installed and running on NetWitness Platform.
- NetWitness Endpoint is installed and running. This is necessary only if you want to configure NetWitness Endpoint as an alert source in the Respond view.

Configure Reporting Engine to Display Reporting Engine Alerts in the Respond View

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

1. Go to **ADMIN > Services**, select a Reporting Engine service, and then select   > **View > Config**.
The Services Config view is displayed with the Reporting Engine General tab open.
2. Select **System Configuration**.

3. Select the checkbox for **Forward Alerts to Respond**.



4. Click **Apply**.

The Reporting Engine now forwards the alerts to NetWitness Respond.

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

Configure Malware Analysis to Display Malware Analysis Alerts in the Respond View

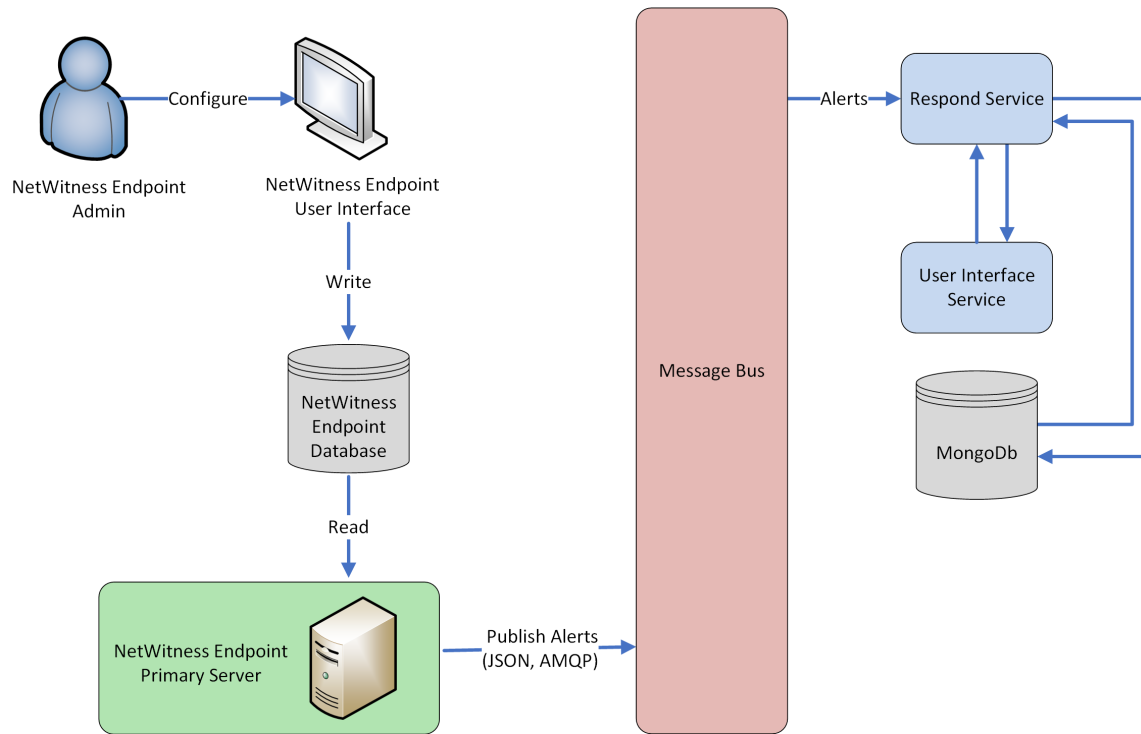
Viewing NetWitness Respond alerts is a function of auditing in Malware Analysis. The procedure for enabling NetWitness Respond alerts is described in the "(Optional) Configure Auditing on Malware Analysis Host" topic in the *Malware Analysis Configuration Guide*.

Configure NetWitness Endpoint to Display NetWitness Endpoint Alerts in the Respond View

This procedure is required to integrate NetWitness Endpoint with NetWitness Platform so that the NetWitness Endpoint alerts are picked up by the NetWitness Respond component of NetWitness Platform and displayed in the **RESPOND > Alerts** view.

Note: RSA supports NetWitness Endpoint versions 4.3.0.4, 4.3.0.5, 4.4, 4.4.0.2, or later for NetWitness Respond integration. For more detailed information, see "RSA NetWitness Endpoint Integration" in the *NetWitness Endpoint User Guide*.

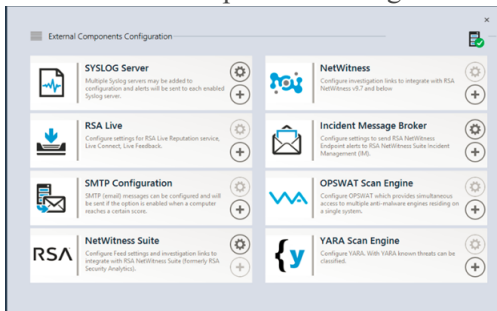
The diagram below represents the flow of NetWitness Endpoint alerts to the NetWitness Platform Respond Server service and its display in the **RESPOND > Alerts** view.



To configure NetWitness Endpoint to display NetWitness Endpoint alerts in the NetWitness Platform user interface:

1. In the NetWitness Endpoint user interface, click **Configure > Monitoring and External Components**.

The External Components Configuration dialog is displayed.



2. From the components listed, select **Incident Message Broker** and click + to add a new IM Broker.
3. Enter the following fields:
 - a. **Instance Name**: Enter a unique name to identify the IM broker.
 - b. **Server Hostname/IP address**: Enter the Host DNS or IP address of the IM Broker (NetWitness Server).
 - c. **Port number**: The default port is 5671.
4. Click **Save**.
5. Navigate to the **ConsoleServer.exe.Config** file in **C:\Program Files\RSA\ECAT\Server**.

6. Modify the virtual host configurations in the file as follows:

```
<add key="IMVirtualHost" value="/rsa/system" />
```

Note: In NetWitness Platform 11.0 and later, the virtual host is “/rsa/system”. For version 10.6.x and below, the virtual host is “/rsa/sa”.

7. Restart the API Server and Console Server.
8. To set up SSL for Respond Alerts, perform the following steps on the NetWitness Endpoint primary console server to set the SSL communications:

- a. Export the NetWitness Endpoint CA certificate to .CER format (Base-64 encoded X.509) from the personal certificate store of the local computer (without selecting the private key).
- b. Generate a client certificate for NetWitness Endpoint using the NetWitness Endpoint CA certificate. (You MUST set the CN name 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 "NWECA" -is MY -ir LocalMachine -sp
"Microsoft RSA SChannel Cryptographic Provider" -cy end -sy 12
client.cer
```

Note: In the above code sample, if you upgraded to Endpoint version 4.3 from a previous version and did not generate new certificates, you should substitute EcatCA for NWECA.

- c. 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"/>
```

9. On the NetWitness Server, copy the NetWitness Endpoint CA certificate file in .CER format into the import folder:
- ```
/etc/pki/nw/trust/import
```
10. Issue the following command to initiate the necessary Chef run:
- ```
orchestration-cli-client --update-admin-node
```
- This appends all of those certificates into the truststore.
11. Restart the RabbitMQ server:
- ```
systemctl restart rabbitmq-server
```
- The NetWitness Endpoint account should automatically be available on RabbitMQ.
12. Import the `/etc/pki/nw/ca/nwca-cert.pem` and `/etc/pki/nw/ca/ssca-cert.pem` files from the NetWitness Server and add them to the Trusted Root Certification stores in the Endpoint Server.

## Step 2. Assign Respond View Permissions

Add users with the required permissions to investigate incidents and alerts in NetWitness Respond. Users with access to the Respond view need both Incidents and Respond-server permissions. Users with access to configure Respond notification settings need additional Integration-server permissions.

The following pre-configured roles have permissions in the Respond view:

- **Analysts:** The Security Operations Center (SOC) Analysts have access to Alerting, NetWitness Respond, Investigate, and Reporting, but not system configurations.
- **Malware Analysts:** Malware Analysts have access to investigations and malware events.
- **Operators:** Operators have access to configurations, but not Investigate, ESA, Alerting, Reporting and NetWitness Respond.
- **SOC\_Managers:** The SOC Managers have the same access as Analysts plus additional permissions to handle incidents and configure NetWitness Respond.
- **Data\_Privacy\_Officers:** Data Privacy Officers (DPOs) are like Administrators with additional focus on configuration options that manage obfuscation and viewing of sensitive data within the system. See the *Data Privacy Management Guide* for additional information.
- **Respond\_Administrator:** The Respond Administrator has full access to NetWitness Respond.
- **Administrators:** The Administrator has full system access to NetWitness Platform and has all permissions by default.

The NetWitness Respond default permissions are shown in the following tables. You need to assign user permissions from both the **Incidents** and **Respond-server** tabs, which are the Permissions tab names in the ADMIN > Security view Add or Edit Roles dialogs. You may want to add additional user permissions for Alerting, Context Hub, Investigate, Investigate-server, and Reports.

**Caution:** It is very important that you assign equivalent user permissions from BOTH the Respond-server tab AND the Incidents tab.

Users who configure Respond notification settings also need permissions in the Integration-server tab.

## Respond-server

| Permissions                                                         | Analysts | SOC Mgrs | DPOs | Respond Admin | Operators | MAs |
|---------------------------------------------------------------------|----------|----------|------|---------------|-----------|-----|
| respond-server.alert.delete                                         |          |          | Yes* | Yes*          |           |     |
| respond-server.alert.manage                                         | Yes      | Yes      | Yes* | Yes*          |           | Yes |
| respond-server.alert.read                                           | Yes      | Yes      | Yes* | Yes*          |           | Yes |
| respond-server.alertrule.manage                                     |          | Yes      | Yes* | Yes*          |           |     |
| respond-server.alertrule.read                                       |          | Yes      | Yes* | Yes*          |           |     |
| respond-server.configuration.manage                                 |          |          | Yes* | Yes*          |           |     |
| respond-server.health.read                                          |          |          | Yes* | Yes*          |           |     |
| respond-server.incident.delete                                      |          |          | Yes* | Yes*          |           |     |
| respond-server.incident.manage                                      | Yes      | Yes      | Yes* | Yes*          |           | Yes |
| respond-server.incident.read                                        | Yes      | Yes      | Yes* | Yes*          |           | Yes |
| respond-server.journal.manage                                       | Yes      | Yes      | Yes* | Yes*          |           | Yes |
| respond-server.journal.read                                         | Yes      | Yes      | Yes* | Yes*          |           | Yes |
| respond-server.logs.manage                                          |          |          | Yes* | Yes*          |           |     |
| respond-server.metrics.read                                         |          |          | Yes* | Yes*          |           |     |
| respond-server.notification.manage<br>(Available in 11.1 and later) |          | Yes      | Yes* | Yes*          |           |     |
| respond-server.notification.read<br>(Available in 11.1 and later)   |          | Yes      | Yes* | Yes*          |           |     |
| respond-server.process.manage                                       |          |          | Yes* | Yes*          |           |     |
| respond-server.remediation.manage                                   | Yes      | Yes      | Yes* | Yes*          |           | Yes |
| respond-server.remediation.read                                     | Yes      | Yes      | Yes* | Yes*          |           | Yes |
| respond-server.risk.manage                                          | Yes      |          | Yes* | Yes*          |           |     |
| respond-server.risk.read                                            | Yes      |          | Yes* | Yes*          |           |     |
| respond-server.security.manage                                      |          |          | Yes* | Yes*          |           |     |
| respond-server.security.read                                        |          |          | Yes* | Yes*          |           |     |

\* Data Privacy Officers and Respond Administrators have the **respond-server.\*** permission, which gives them all of the Respond-server permissions.

## Incidents

| Permissions                               | Analysts | SOC Mgrs | DPOs | Respond Admin | Operators | MAs |
|-------------------------------------------|----------|----------|------|---------------|-----------|-----|
| Access Incident Module                    | Yes      | Yes      | Yes  | Yes           |           | Yes |
| Configure Incident Management Integration |          | Yes      | Yes  | Yes           |           |     |
| Delete Alerts and Incidents               |          |          | Yes  | Yes           |           |     |
| Manage Alert Handling Rules               |          | Yes      | Yes  | Yes           |           |     |
| View and Manage Incidents                 | Yes      | Yes      | Yes  | Yes           |           | Yes |

The Respond Administrator has all of the Respond-server and Incidents permissions.

## Integration-server

**Note:** The Integration-server permissions are available in NetWitness Platform version 11.1 and later.

Users who configure Respond Notifications also need Integration-server permissions. The following table lists the Respond Notification setting permissions in the Integration-server tab assigned to each role.

| Permissions                            | Analysts | SOC Mgrs | DPOs | Respond Admin | Operators | MAs |
|----------------------------------------|----------|----------|------|---------------|-----------|-----|
| integration-server.notification.read   |          | Yes      | Yes  | Yes           |           |     |
| integration-server.notification.manage |          | Yes      | Yes  | Yes           |           |     |

## Investigate-server

Users who view Event Analysis in Respond also need Investigate-server permissions. The following table lists the Respond Event Analysis permissions required in the Investigate-server tab and the permissions assigned to each role.

| Permissions                            | Analysts | SOC Mgrs | DPOs | Respond Admin | Operators | MAs |
|----------------------------------------|----------|----------|------|---------------|-----------|-----|
| investigate-server.event.read          | Yes      | Yes      | Yes  | Yes           |           | Yes |
| investigate-server.content.reconstruct | Yes      | Yes      | Yes  | Yes           |           | Yes |
| investigate-server.content.export      | Yes      | Yes      | Yes  | Yes           |           | Yes |



## Respond Notification Settings Permissions

**Note:** The Respond notification setting permissions are available in NetWitness Platform version 11.1 and later.

If you are updating from NetWitness Platform version 11.0 to 11.1 or later, you will need to add additional permissions to your existing built-in NetWitness Platform user roles. For all upgrades to 11.1 or later, you will need to add additional permissions to custom roles.

The following permissions are required for Respond Administrators, Data Privacy Officers, and SOC Managers to access Respond Notification Settings (CONFIGURE > Respond Notifications).

Incidents tab:

- Configure Incident Management Integration

Respond-server tab:

- respond-server.notification.manage
- respond-server.notification.read

Integration-server tab:

- integration-server.notification.read
- integration-server.notification.manage

## Respond Event Analysis Permissions

**Note:** The Event Analysis panel in the Respond view is available in NetWitness Platform version 11.2 and later.

The Event Analysis panel in the Respond view shows the Event Analysis view from Investigate for specific indicator events. The following permissions are required to view Event Analysis in the Respond view. These permissions are provided by default for users with the Analysts role.

Investigate-server tab:

- investigate-server.event.read
- investigate-server.content.reconstruct
- investigate-server.content.export

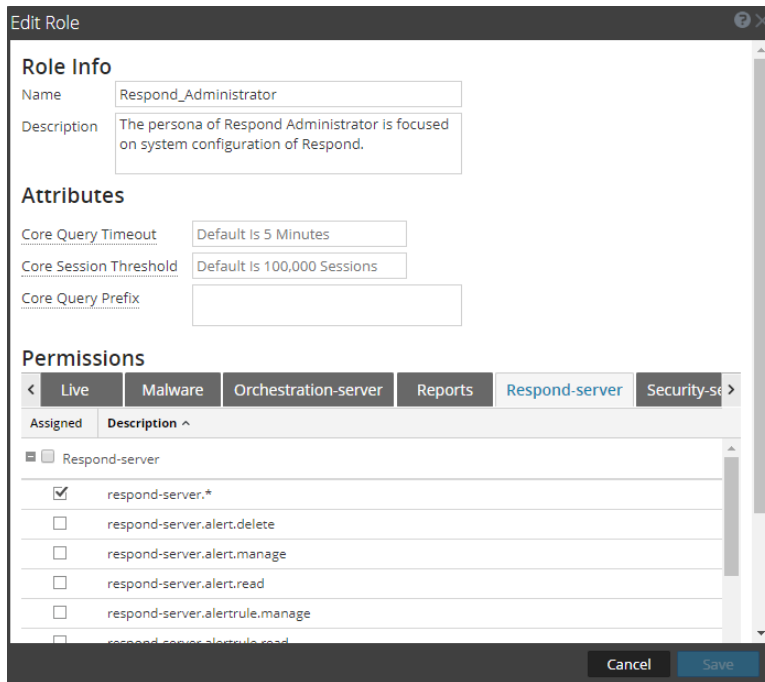
Administration tab:

- Access Administration Module

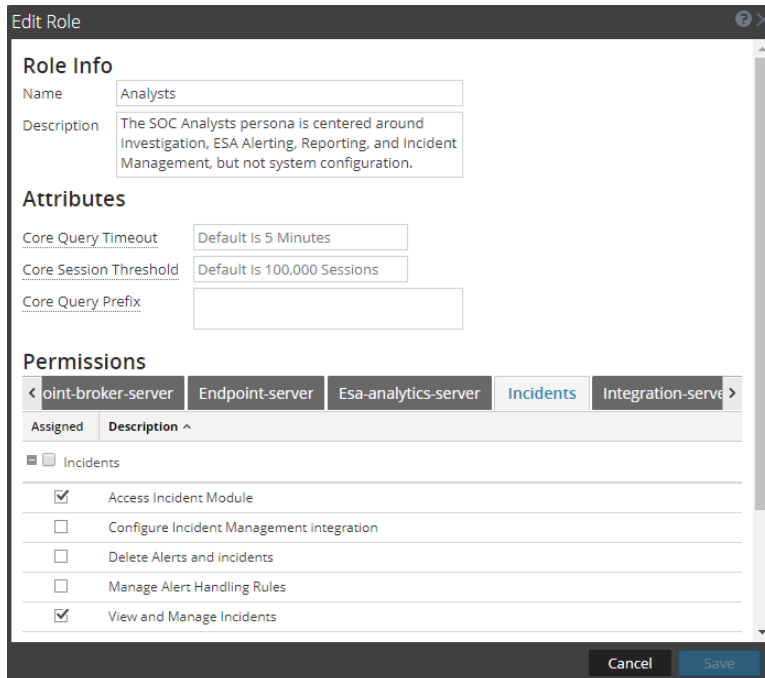
**Note:** Migrated incidents from NetWitness Platform versions before 11.2 will not show the Event Analysis panel in the Respond Incident Details view Indicators panel. Likewise, if you use alerts that were migrated from versions before 11.2 to create incidents in 11.2, you will also not be able to view the Event Analysis panel in the Respond view for those incidents.

## Respond Role Permission Examples

The following figure shows Respond-server permissions for the default Respond Administrator role. The Respond Administrator role contains all of the NetWitness Respond permissions.



The following figure shows the Incidents permissions for the default Analysts role:



For more information, see "Role Permissions" and "Manage Users with Roles and Permissions" in the *System Security and User Management* guide.

## Step 3. Enable and Create Incident Rules for Alerts

NetWitness Respond incident rules contain criteria to automate the process of creating incidents from alerts. Alerts that meet the rule criteria are grouped together to form an incident. Analysts use these incidents to locate indicators of compromise. Instead of creating an incident for a particular set of alerts and adding the alerts to that incident manually, you can save time by using incident rules to create incidents from alerts for you.

NetWitness Platform provides predefined incident rules that you can use and you can also create your own rules based on your business requirements.

To create incidents automatically, you need to enable at least one incident rule.

When you have two or more incident rules enabled, the order of the rules becomes very important. The highest priority rules are at the top of the Incident Rules list. The highest priority rule has the number 1 in the Order field. The next highest priority rule is number 2 in the Order field, and so on. Alerts can only be part of one incident. If an alert matches more than one rule in the Incident Rule list, it is only evaluated using the highest priority rule that it matches.

NetWitness Platform has 13 predefined incident rules that you can use. To set up your incident rules, you can do any of the following:

- Enable predefined incident rules
- Add new rules
- Clone rules
- Edit existing rules

The User Entity Behavior Analytics incident rule is available in 11.3 and later. It captures user entity behavior grouped by Classifier ID to create incidents from alerts. The User Behavior default incident rule is available in NetWitness Platform 11.1 and later. It captures network user behavior and uses deployed RSA Live ESA Rules to create incidents from alerts.

You can select and deploy the RSA Live ESA Rules that you want to monitor. For more information, see [Deploy the RSA Live ESA Rules](#).

Some predefined (default) incident rules changed slightly in 11.1 and later. To verify your existing default incident rules with the 11.3 default incident rules, see [Set Up and Verify Default Incident Rules](#).

### Enable an Incident Rule

To create incidents automatically, you need to enable at least one incident rule. Predefined (default) incident rules or rules that you create must be enabled before they start creating incidents.

1. Go to **CONFIGURE > Incident Rules**.  
The Incident Rules view is displayed.

| SELECT                | ORDER | ENABLED                             | NAME                                                   | DESCRIPTION                                          | LAST MATCHED | MATCHED ALERTS | INCIDENTS |
|-----------------------|-------|-------------------------------------|--------------------------------------------------------|------------------------------------------------------|--------------|----------------|-----------|
| <input type="radio"/> | 1     | <input checked="" type="checkbox"/> | User Behavior                                          | This incident rule captures network user beha...     |              | 0              | 0         |
| <input type="radio"/> | 2     | <input checked="" type="checkbox"/> | Suspected Command & Control Communication By Domain    | This incident rule captures suspected commun...      |              | 0              | 0         |
| <input type="radio"/> | 3     | <input checked="" type="checkbox"/> | High Risk Alerts: Malware Analysis                     | This incident rule captures alerts generated by...   |              | 0              | 0         |
| <input type="radio"/> | 4     | <input checked="" type="checkbox"/> | High Risk Alerts: NetWitness Endpoint                  | This incident rule captures alerts generated by...   |              | 0              | 0         |
| <input type="radio"/> | 5     | <input checked="" type="checkbox"/> | High Risk Alerts: Reporting Engine                     | This incident rule captures alerts generated by...   |              | 0              | 0         |
| <input type="radio"/> | 6     | <input checked="" type="checkbox"/> | High Risk Alerts: ESA                                  | This incident rule captures alerts generated by...   |              | 0              | 0         |
| <input type="radio"/> | 7     | <input checked="" type="checkbox"/> | IP Watch List: Activity Detected                       | This incident rule captures alerts generated by...   |              | 0              | 0         |
| <input type="radio"/> | 8     | <input checked="" type="checkbox"/> | User Watch List: Activity Detected                     | This incident rule captures alerts generated by...   |              | 0              | 0         |
| <input type="radio"/> | 9     | <input checked="" type="checkbox"/> | Suspicious Activity Detected: Windows Worm Propagation | This incident rule captures alerts that are indic... |              | 0              | 0         |
| <input type="radio"/> | 10    | <input checked="" type="checkbox"/> | Suspicious Activity Detected: Reconnaissance           | This incident rule captures alerts that identify ... |              | 0              | 0         |
| <input type="radio"/> | 11    | <input checked="" type="checkbox"/> | Monitoring Failure: Device Not Reporting               | This incident rule captures any instance of an ...   |              | 0              | 0         |
| <input type="radio"/> | 12    | <input checked="" type="checkbox"/> | Web Threat Detection                                   | This incident rule captures alerts generated by...   |              | 0              | 0         |
| <input type="radio"/> | 13    | <input checked="" type="checkbox"/> | User Entity Behavior Analytics                         | This incident rule captures user entity behavior.    |              | 0              | 0         |

- Click the link in the **Name** column for the rule that you want to enable. The Incident Rule Details view is displayed for the selected rule.

**BASIC SETTINGS**  **ENABLED**

**NAME\***  
High Risk Alerts: Malware Analysis

**DESCRIPTION**  
This incident rule captures alerts generated by the RSA Malware Analysis platform as having a Risk Score of "High" or "Critical".

**MATCH CONDITIONS\***  
QUERY MODE: Rule Builder

Grouping: All of these

| FIELD      | OPERATOR                 | VALUE            |
|------------|--------------------------|------------------|
| Source     | is equal to              | Malware Analysis |
| Risk Score | is equal or greater than | 50               |

**ACTION\***  
CHOOSE THE ACTION TAKEN IF THE RULE MATCHES AN ALERT  
 Group into an Incident  Suppress the Alert

**GROUPING OPTIONS**  
 GROUP BY\*: Source IP Address  
 TIME WINDOW: 1 Hours



**INCIDENT OPTIONS**  
 TITLE\*: \${ruleName} for \${groupByValue}  
 SUMMARY: Enter a summary for the incident created by this rule  
 CATEGORIES: Choose a category (optional)  
 ASSIGNEE: Choose an assignee (optional)  
 PRIORITY: Use the following to set the priority for the 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

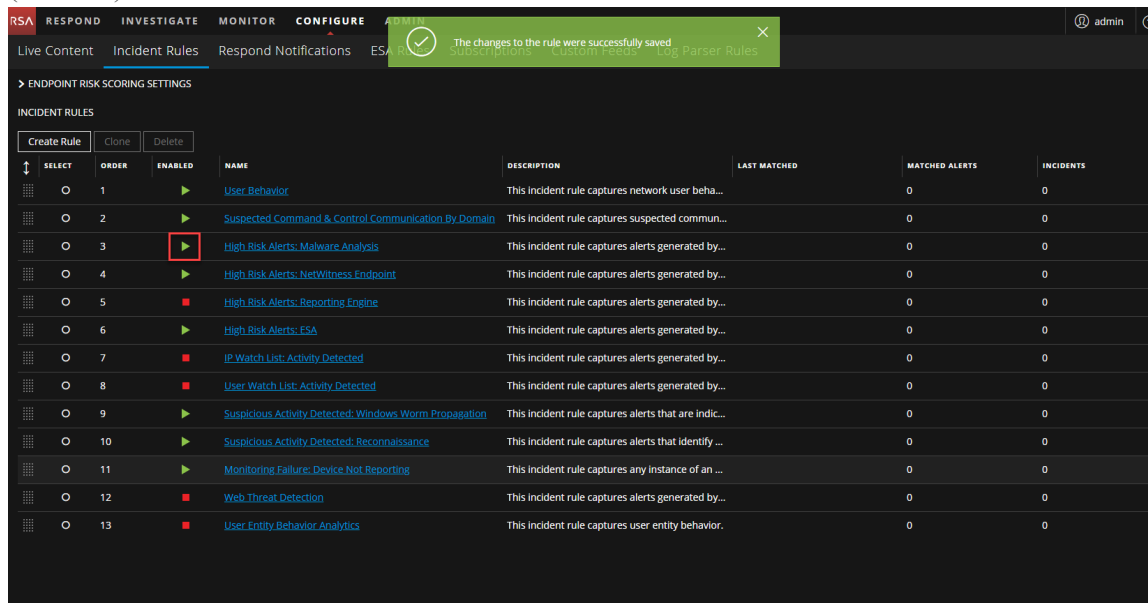
Priority Legend:  
 Critical: 90  
 High: 50  
 Medium: 20  
 Low: 1

Buttons: Cancel, Save

- Adjust the parameters and conditions of your rule as required. For details about various parameters that can be set as criteria for an incident rule, see [Incident Rule Details View](#).
- In the Basic Settings section, select **Enabled**.

- Click **Save** to enable the rule.

Notice that the Enabled column changes from a red square  (Disabled) to green triangle  (Enabled).

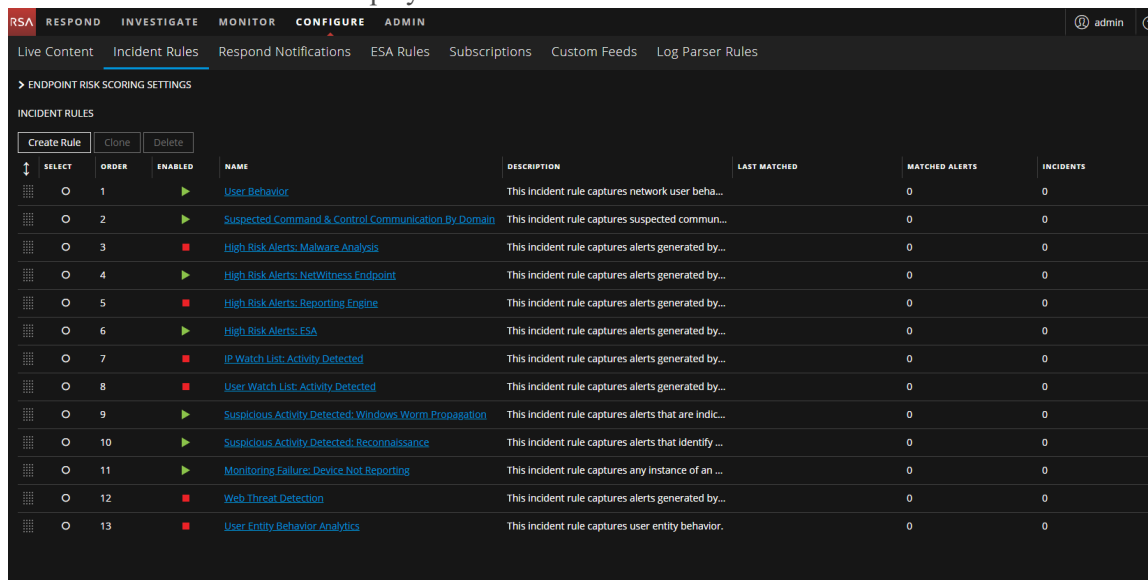


- Verify the order of your incident rules.

## Create an Incident Rule

- Go to **CONFIGURE > Incident Rules**.

The Incident Rules view is displayed.



- To add a new rule, click **Create Rule**.

The Incident Rule Details view is displayed.

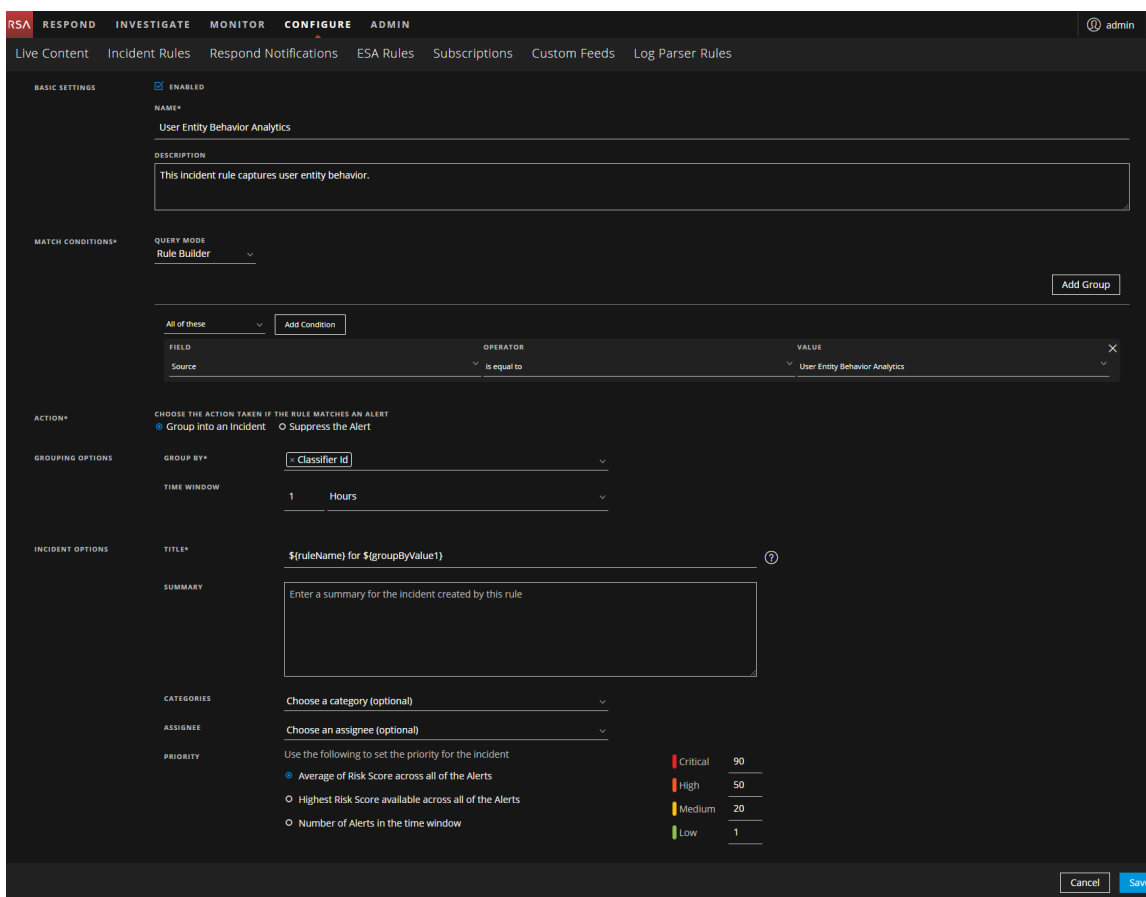
The screenshot shows the 'Incident Rule Details' configuration page in NetWitness Respond. The page is divided into several sections:

- BASIC SETTINGS:** Includes an 'ENABLED' checkbox, a 'NAME\*' field with a placeholder 'Provide a unique name for the rule', and a 'DESCRIPTION' field with a placeholder 'Provide a description of the rule'.
- MATCH CONDITIONS\*:** Features a 'QUERY MODE' dropdown set to 'Rule Builder', an 'Add Group' button, and a list of conditions. A dropdown menu is open showing a 'FIELD' selection. A warning message states: 'At least one condition is missing a field, operator, or value'.
- ACTION\*:** Under the heading 'CHOOSE THE ACTION TAKEN IF THE RULE MATCHES AN ALERT', there are two radio buttons: 'Group into an Incident' (selected) and 'Suppress the Alert'.
- GROUPING OPTIONS:** Includes a 'GROUP BY\*' dropdown with the text 'Choose a group-by field (required)' and a warning: 'A MINIMUM OF ONE GROUP-BY FIELD IS REQUIRED, AND A MAXIMUM OF TWO IS ALLOWED'. Below it is a 'TIME WINDOW' dropdown set to '1 Hours'.
- INCIDENT OPTIONS:** Includes a 'TITLE\*' field with the placeholder '\$ruleName) for \$(groupByValue1)' and a 'SUMMARY' field with the placeholder 'Enter a summary for the incident created by this rule'.

At the bottom of the page, there is a yellow warning triangle with the text 'There is required information missing from the incident rule' and 'Cancel' and 'Save' buttons.

3. Enter the parameters and conditions of your rule. All rules need to have at least one condition. For details about parameters that can be set as criteria for an incident rule, see [Incident Rule Details View](#).

The following figure shows a rule example.



4. If you are ready to enable your rule, in the Basic Settings section, select **Enabled**.
5. Click **Save**.

The rule appears in the Incidents Rules list. If you selected Enabled, the rule is enabled and it starts creating incidents depending on the incoming alerts that match the selected criteria.

6. Verify the order of your incident rules.

## Verify the Order of Your Incident Rules

NetWitness Respond evaluates incoming alerts against the incident rules in the order that you define. If alerts match the first rule listed, then that rule creates an incident. If alerts match the second rule listed and those alerts did not match the first rule, then the second rule creates an incident. If alerts match the third rule listed and those alerts did not match the first or second rule listed, then the third rule creates an incident, and so on.

To change the order of the rules, use the drag pads (  ) in front of the rules to move them up and down in the list.

The rule order determines which rule takes effect if the criteria for multiple rules match the same alert. If multiple rules match an alert, only the rule with the highest priority creates an incident.

## Clone an Incident Rule

It is often easier to duplicate an existing rule that is similar to a rule that you want to create and adjust it accordingly.

1. Go to **CONFIGURE > Incident Rules**.  
The Incident Rules view is displayed.
2. Select the rule that you would like to copy and click **Clone**.
3. Adjust the parameters and conditions of your rule as required. All rules need to have at least one condition.
4. If you are ready to enable your rule, in the Basic Settings section, select **Enabled**.
5. Click **Save** to create the rule.
6. Verify the order of your incident rules.

## Edit an Incident Rule

1. Go to **CONFIGURE > Incident Rules** and click the link in the **Name** column for the rule that you want to update.  
The Incident Rule Details view is displayed.
2. Adjust the parameters and conditions of your rule as required. All rules need to have at least one condition.
3. If you are ready to enable your rule, in the Basic Settings section, select **Enabled**.
4. Click **Save** to update the rule.
5. Verify the order of your incident rules.

### See Also:

- For details about parameters that can be set as criteria for an incident rule, see [Incident Rule Details View](#).
- For details on the parameter and field descriptions in the Incident Rules list, see [Incident Rules View](#).



## Additional Procedures for Respond Configuration

---

Use this section when you are looking for instructions to perform a specific task after the initial setup of NetWitness Respond.

- [Set Up and Verify Default Incident Rules](#)
- [Configure Risk Scoring Settings for Automated Incident Creation](#)
- [Configure Respond Email Notification Settings](#)
- [Set a Retention Period for Alerts and Incidents](#)
- [Obfuscate Private Data](#)
- [Manage Incidents in Archer Cyber Incident & Breach Response](#)
- [Configure the Option to Send Incidents to RSA Archer](#)
- [Configure Threat Aware Authentication](#)
- [Set Counter for Matched Alerts and Incidents](#)
- [Configure a Database for the Respond Server Service](#)

## Set Up and Verify Default Incident Rules

A User Entity Behavior Analytics default incident rule is available in NetWitness Platform 11.3 and later. It captures user entity behavior grouped by Classifier ID to create incidents from alerts.

A User Behavior incident rule, which captures network user behavior, is available in NetWitness Platform 11.1 and later. This rule uses deployed RSA Live ESA Rules to create incidents from alerts. You can select and deploy the RSA Live ESA Rules that you want to monitor.

The following default incident rules changed slightly for 11.1 and later and now have **Source IP Address** as the Group By value:

- High Risk Alerts: Reporting Engine
- High Risk Alerts: Malware Analysis
- High Risk Alerts: ESA

The following default incident rule changed slightly for 11.3 and now has the **Host Name** as the Group By value:

- High Risk Alerts: NetWitness Endpoint\*

\*If you have NetWitness Endpoint, the High Risk Alerts: NetWitness Endpoint default incident rule captures alerts generated by NetWitness Endpoint with a risk score of High or Critical. To aggregate NetWitness Endpoint alerts based on the File Hash instead of Host Name, create another NetWitness Endpoint Rule using the File Hash as the Group By value. See [Create a NetWitness Endpoint Incident Rule using File Hash](#) for step-by-step instructions.

To verify your existing default incident rules with the 11.3 default incident rules, look at the default incident rule tables following these procedures. If you are missing a default incident rule, you can create it manually. Review the default incident rules and adjust them to your environment as required.


## Set Up the User Behavior Incident Rule

In order to use the default User Behavior incident rule, you need to deploy the RSA Live ESA Rules that you want to monitor from those listed in the User Behavior incident rule conditions. Complete the following procedures to start aggregating alerts for the User Behavior default incident rule:

- Deploy the RSA Live ESA Rules
- Adjust and enable the User Behavior default rule (or create it if you do not have it)

### Deploy the RSA Live ESA Rules

1. Go to **CONFIGURE > Live Content**.
2. In the **Resource Types** field, select **Event Steam Analysis Rule** and click **Search**.
3. In the **Matching Resources** list, select the ESA Rules from the following **User Behavior** table that you are interested in monitoring and deploy them (click **Deploy**).
4. Go to **CONFIGURE > ESA Rules > Rules** tab, and in the Rule Library **Filter** drop-down list, select **RSA Live ESA Rule**.

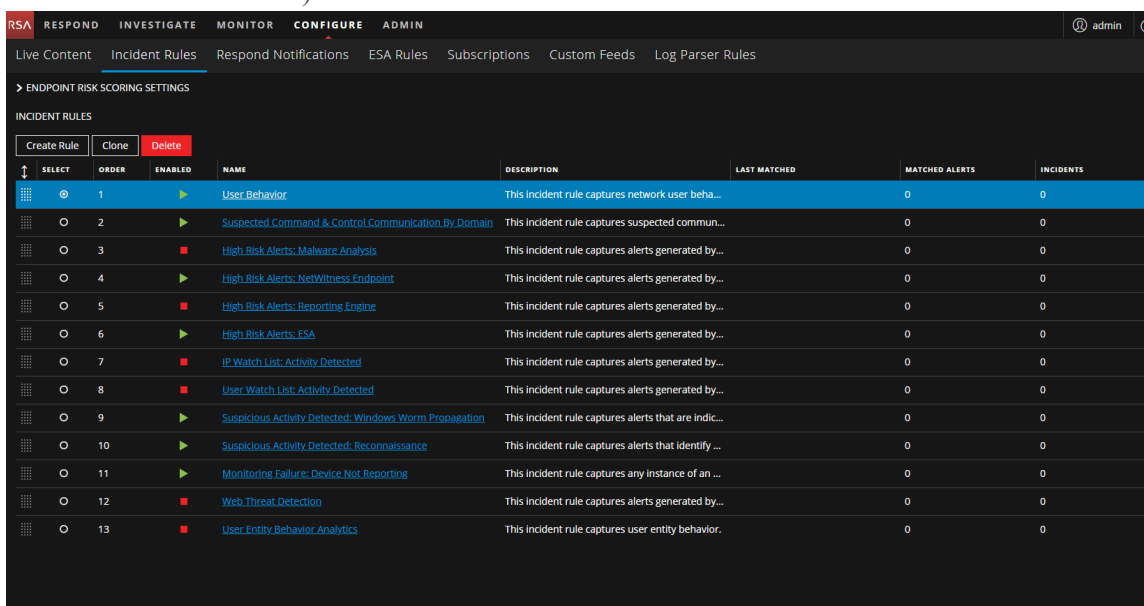
5. To add a new Deployment, in the drop-down list near **DEPLOYMENTS**, click **Add**.
  - a. In the ESA Services section, add and then select your ESA service.
  - b. In the ESA Rules section, click  and in the Deploy ESA Rules dialog, select the ESA Rules that you selected from the **User Behavior** table, and then click **Save**.  
The selected ESA rules are listed with a status of **Added**.
6. Select the ESA rules that you added from the previous step, and click **Deploy Now**.  
The status of the selected ESA rules changes to **Deployed**.
7. Go to **CONFIGURE > ESA Rules > Services** tab.  
In the **Deployed Rule Stats** for your ESA service, the rules that you added should have a status of enabled, which is indicated by a green circle in the Enable column.

### Adjust and Enable the User Behavior Default Rule (or Create It If You Do Not Have It)

If you have the User Behavior default rule, you can adjust it for your environment and enable it. If you do not have the User Behavior default rule, you can create it manually.

#### (Optional) To create the User Behavior default rule:

1. Go to **CONFIGURE > Incident Rules**.  
The Incident Rules view is displayed. (The following figure shows what the User Behavior rule looks like if it was there.)



| SELECT | ORDER | ENABLED | NAME                                                   | DESCRIPTION                                          | LAST MATCHED | MATCHED ALERTS | INCIDENTS |
|--------|-------|---------|--------------------------------------------------------|------------------------------------------------------|--------------|----------------|-----------|
|        | 1     |         | User Behavior                                          | This incident rule captures network user beha...     |              | 0              | 0         |
|        | 2     |         | Suspected Command & Control Communication By Domain    | This incident rule captures suspected commun...      |              | 0              | 0         |
|        | 3     |         | High Risk Alerts: Malware Analysis                     | This incident rule captures alerts generated by...   |              | 0              | 0         |
|        | 4     |         | High Risk Alerts: NetWitness Endpoint                  | This incident rule captures alerts generated by...   |              | 0              | 0         |
|        | 5     |         | High Risk Alerts: Reporting Engine                     | This incident rule captures alerts generated by...   |              | 0              | 0         |
|        | 6     |         | High Risk Alerts: ESA                                  | This incident rule captures alerts generated by...   |              | 0              | 0         |
|        | 7     |         | IP Watch List: Activity Detected                       | This incident rule captures alerts generated by...   |              | 0              | 0         |
|        | 8     |         | User Watch List: Activity Detected                     | This incident rule captures alerts generated by...   |              | 0              | 0         |
|        | 9     |         | Suspicious Activity Detected: Windows Worm Propagation | This incident rule captures alerts that are indic... |              | 0              | 0         |
|        | 10    |         | Suspicious Activity Detected: Reconnaissance           | This incident rule captures alerts that identify ... |              | 0              | 0         |
|        | 11    |         | Monitoring Failure: Device Not Reporting               | This incident rule captures any instance of an ...   |              | 0              | 0         |
|        | 12    |         | Web Threat Detection                                   | This incident rule captures alerts generated by...   |              | 0              | 0         |
|        | 13    |         | User Entity Behavior Analytics                         | This incident rule captures user entity behavior.    |              | 0              | 0         |

2. Click **Create Rule** and in the Incident Rule Details view, create the User Behavior default incident rule using the values in the User Behavior table following this procedure. Values not listed in the table should be set for your business requirements. For details about various parameters that can be set as criteria for an incident rule, see [Incident Rule Details View](#).

The following figure shows a portion of the User Behavior default rule details. Notice that there are

two groups in this rule.

The screenshot shows the NetWitness Respond Configuration interface. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The 'CONFIGURE' tab is active, and the 'Incident Rules' sub-tab is selected. The rule being configured is named 'User Behavior' and is currently 'ENABLED'. The description is 'This incident rule captures network user behavior.' The 'MATCH CONDITIONS\*' section is set to 'Rule Builder' and 'All of these'. The conditions are as follows:

| GROUP        | FIELD      | OPERATOR    | VALUE                                                       |
|--------------|------------|-------------|-------------------------------------------------------------|
| All of these | Source     | is equal to | Event Stream Analysis                                       |
| Any of these | Alert Name | is equal to | Account Added to Administrators Group and Removed           |
| Any of these | Alert Name | is equal to | Account Removals From Protected Groups on Domain Controller |
| Any of these | Alert Name | is equal to | Detects Router Configuration Attempts                       |
| Any of these | Alert Name | is equal to | Direct Login By A Guest Account                             |
| Any of these | Alert Name | is equal to | Direct Login to an Administrative Account                   |
| Any of these | Alert Name | is equal to | Failed Logins Followed By Successful Login Password Change  |

Buttons for 'Add Condition', 'Add Group', 'Remove Group', 'Cancel', and 'Save' are visible.

3. If you are ready to enable your rule, in the Basic Settings section, select **Enabled**.
4. Click **Save**.  
The rule appears in the Incidents Rules list. If you selected Enabled, the rule is enabled and it starts creating incidents depending on the incoming alerts that are matched as per the rule criteria.
5. Verify the order of your incident rules. For more information, see [Verify the Order of Your Incident Rules](#).

## User Behavior

The following table shows the values for the User Behavior default incident rule.

| Field       | Condition Field | Condition Operator | Value                                                                      |
|-------------|-----------------|--------------------|----------------------------------------------------------------------------|
| Name        |                 |                    | User Behavior                                                              |
| Description |                 |                    | This incident rule captures network user behavior.                         |
| 1st Group:  |                 |                    | All of these                                                               |
| Condition:  | Source          | is equal to        | Event Stream Analysis                                                      |
| 2nd Group:  |                 |                    | Any of these                                                               |
| Conditions: | Alert Name      | is equal to        | Account Added to Administrators Group and Removed                          |
|             | Alert Name      | is equal to        | Account Removals From Protected Groups on Domain Controller                |
|             | Alert Name      | is equal to        | Detects Router Configuration Attempts                                      |
|             | Alert Name      | is equal to        | Direct Login By A Guest Account                                            |
|             | Alert Name      | is equal to        | Direct Login to an Administrative Account                                  |
|             | Alert Name      | is equal to        | Failed Logins Followed By Successful Login Password Change                 |
|             | Alert Name      | is equal to        | Insider Threat Mass Audit Clearing                                         |
|             | Alert Name      | is equal to        | Internal Data Posting to 3rd Party Sites                                   |
|             | Alert Name      | is equal to        | kbrtgt Account Modified on Domain controller                               |
|             | Alert Name      | is equal to        | Lateral Movement Suspected Windows                                         |
|             | Alert Name      | is equal to        | Logins across Multiple Servers                                             |
|             | Alert Name      | is equal to        | Logins by Same User to Multiple Servers                                    |
|             | Alert Name      | is equal to        | Malicious Account Creation Followed by Failed Authorization                |
|             | Alert Name      | is equal to        | Multiple Account Lockouts From Same or Different Users                     |
|             | Alert Name      | is equal to        | Multiple Failed Logins Followed By a Successful Login                      |
|             | Alert Name      | is equal to        | Multiple Failed Logins from Same User Originating from Different Countries |
|             | Alert Name      | is equal to        | Multiple Failed Privilege Escalations by Same User                         |
|             | Alert Name      | is equal to        | Multiple Intrusion Scan Events from Same User to Unique Destinations       |

| Field       | Condition Field | Condition Operator | Value                                                            |
|-------------|-----------------|--------------------|------------------------------------------------------------------|
|             | Alert Name      | is equal to        | Multiple Login Failures by Administrators to Domain Controller   |
|             | Alert Name      | is equal to        | Multiple Login Failures by Guest to Domain Controller            |
|             | Alert Name      | is equal to        | Multiple Failed Logons from Same Source IP with Unique Usernames |
|             | Alert Name      | is equal to        | Multiple Successful Logins from Multiple Diff Src to Diff Dest   |
|             | Alert Name      | is equal to        | Multiple Successful Logins from Multiple Diff Src to Same Dest   |
|             | Alert Name      | is equal to        | Privilege Escalation Detected                                    |
|             | Alert Name      | is equal to        | Privilege Escalation Detected in Unix                            |
|             | Alert Name      | is equal to        | Privilege User Account Password Change                           |
|             | Alert Name      | is equal to        | Failed Logins Outside Business Hours                             |
|             | Alert Name      | is equal to        | DNS Tunneling                                                    |
|             | Alert Name      | is equal to        | User Login Baseline                                              |
| Group By    |                 |                    | Destination User Account                                         |
| Time Window |                 |                    | 1 Hour                                                           |
| Title       |                 |                    | \${ruleName} for \${groupByValue1}                               |

## Set up or Verify a Default Incident Rule

1. Go to **CONFIGURE > Incident Rules**.  
The Incident Rules view is displayed.

The screenshot shows the NetWitness Respond configuration interface. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The 'CONFIGURE' tab is active, and the 'Incident Rules' sub-tab is selected. Below the navigation, there are links for 'Live Content', 'Incident Rules', 'Respond Notifications', 'ESA Rules', 'Subscriptions', 'Custom Feeds', and 'Log Parser Rules'. The main content area is titled 'ENDPOINT RISK SCORING SETTINGS' and contains a table of 'INCIDENT RULES'. The table has columns for 'SELECT', 'ORDER', 'ENABLED', 'NAME', 'DESCRIPTION', 'LAST MATCHED', 'MATCHED ALERTS', and 'INCIDENTS'. There are 13 rows of incident rules, each with a unique name and description. The 'ENABLED' column contains green play icons for rules 1, 2, 4, 6, 7, 9, 10, and 11, and red square icons for rules 3, 5, 8, 12, and 13.

| SELECT                | ORDER | ENABLED | NAME                                                   | DESCRIPTION                                          | LAST MATCHED | MATCHED ALERTS | INCIDENTS |
|-----------------------|-------|---------|--------------------------------------------------------|------------------------------------------------------|--------------|----------------|-----------|
| <input type="radio"/> | 1     | ▶       | User Behavior                                          | This incident rule captures network user beha...     |              | 0              | 0         |
| <input type="radio"/> | 2     | ▶       | Suspected Command & Control Communication By Domain    | This incident rule captures suspected commun...      |              | 0              | 0         |
| <input type="radio"/> | 3     | ■       | High Risk Alerts: Malware Analysis                     | This incident rule captures alerts generated by...   |              | 0              | 0         |
| <input type="radio"/> | 4     | ▶       | High Risk Alerts: NetWitness Endpoint                  | This incident rule captures alerts generated by...   |              | 0              | 0         |
| <input type="radio"/> | 5     | ■       | High Risk Alerts: Reporting Engine                     | This incident rule captures alerts generated by...   |              | 0              | 0         |
| <input type="radio"/> | 6     | ▶       | High Risk Alerts: ESA                                  | This incident rule captures alerts generated by...   |              | 0              | 0         |
| <input type="radio"/> | 7     | ▶       | IP Watch List: Activity Detected                       | This incident rule captures alerts generated by...   |              | 0              | 0         |
| <input type="radio"/> | 8     | ■       | User Watch List: Activity Detected                     | This incident rule captures alerts generated by...   |              | 0              | 0         |
| <input type="radio"/> | 9     | ▶       | Suspicious Activity Detected: Windows Worm Propagation | This incident rule captures alerts that are indic... |              | 0              | 0         |
| <input type="radio"/> | 10    | ▶       | Suspicious Activity Detected: Reconnaissance           | This incident rule captures alerts that identify ... |              | 0              | 0         |
| <input type="radio"/> | 11    | ▶       | Monitoring Failure: Device Not Reporting               | This incident rule captures any instance of an ...   |              | 0              | 0         |
| <input type="radio"/> | 12    | ■       | Web Threat Detection                                   | This incident rule captures alerts generated by...   |              | 0              | 0         |
| <input type="radio"/> | 13    | ■       | User Entity Behavior Analytics                         | This incident rule captures user entity behavior.    |              | 0              | 0         |

2. Click the link in the **Name** field of a default incident rule to view the Incident Rule Details view. Set up or verify the default incident rule using the values in the default incident rules tables in this topic. Values not listed in the tables should be set for your business requirements. For details about various parameters that can be set as criteria for an incident rule, see [Incident Rule Details View](#).
3. When you are ready to enable your rule, in the Basic Settings section, select **Enabled**.
4. Click **Save**.
5. Verify the order of your incident rules. For more information, see [Verify the Order of Your Incident Rules](#).

### Suspected Command & Control Communication By Domain

The following table shows the values for the Suspected Command & Control Communication By Domain default incident rule.

| Field       | Condition Field | Condition Operator | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------|-----------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name        |                 |                    | Suspected Command & Control Communication By Domain                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Description |                 |                    | This incident rule captures suspected communication with a Command & Control server and groups results by domain.                                                                                                                                                                                                                                                                                                                                                                                                           |
| Group:      |                 |                    | All of these                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Conditions: | Source          | is equal to        | Event Stream Analysis                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|             | Alert Rule Id   | is equal to        | Suspected C&C                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Group By    |                 |                    | Domain for Suspected C& C                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Time Window |                 |                    | 7 Days                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Title       |                 |                    | Suspected C&C with \${groupByValue1}                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Summary     |                 |                    | <p>NetWitness Platform detected communications with \${groupByValue1} that may be command and control malware.</p> <ol style="list-style-type: none"> <li>1. Evaluate if the domain is legitimate (online radio, news feed, partner, automated testing, etc.).</li> <li>2. Review the domain registration for suspect information (Registrant country, registrar, no registration data found, etc).</li> <li>3. If the domain is suspect, go to the Investigation module to locate other activity to or from it.</li> </ol> |



### High Risk Alerts: Malware Analysis

The following table shows the values for the High Risk Alerts: Malware Analysis default incident rule.

| Field       | Condition Field | Condition Operator       | Value                                                                                                                             |
|-------------|-----------------|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Name        |                 |                          | High Risk Alerts: Malware Analysis                                                                                                |
| Description |                 |                          | This incident rule captures alerts generated by the RSA Malware Analysis platform as having a Risk Score of "High" or "Critical". |
| Group:      |                 |                          | All of these                                                                                                                      |
| Conditions: | Source          | is equal to              | Malware Analysis                                                                                                                  |
|             | Risk Score      | is equal or greater than | 50                                                                                                                                |
| Group By    |                 |                          | Source IP Address                                                                                                                 |
| Time Window |                 |                          | 1 Hour                                                                                                                            |
| Title       |                 |                          | \${ruleName} for \${groupByValue1}                                                                                                |

### High Risk Alerts: NetWitness Endpoint

The following table shows the values for the High Risk Alerts: NetWitness Endpoint default incident rule.

| Field       | Condition Field | Condition Operator       | Value                                                                                                                                |
|-------------|-----------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Name        |                 |                          | High Risk Alerts: NetWitness Endpoint                                                                                                |
| Description |                 |                          | This incident rule captures alerts generated by the RSA NetWitness Endpoint platform as having a Risk Score of "High" or "Critical". |
| Group:      |                 |                          | All of these                                                                                                                         |
| Conditions: | Source          | is equal to              | NetWitness Endpoint                                                                                                                  |
|             | Risk Score      | is equal or greater than | 50                                                                                                                                   |
| Group By    |                 |                          | Host Name*                                                                                                                           |
| Time Window |                 |                          | 1 Hour                                                                                                                               |

| Field | Condition Field | Condition Operator | Value                              |
|-------|-----------------|--------------------|------------------------------------|
| Title |                 |                    | \${ruleName} for \${groupByValue1} |

\*To aggregate NetWitness Endpoint alerts based on the File Hash, create another NetWitness Endpoint Rule using the File Hash as the Group By value. See [Create a NetWitness Endpoint Incident Rule using File Hash](#) for step-by-step instructions.

### High Risk Alerts: Reporting Engine

The following table shows the values for the High Risk Alerts: Reporting Engine default incident rule.

| Field       | Condition Field | Condition Operator       | Value                                                                                                                    |
|-------------|-----------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Name        |                 |                          | High Risk Alerts: Reporting Engine                                                                                       |
| Description |                 |                          | This incident rule captures alerts generated by the RSA Reporting Engine as having a Risk Score of "High" or "Critical". |
| Group:      |                 |                          | All of these                                                                                                             |
| Conditions: | Source          | is equal to              | Reporting Engine                                                                                                         |
|             | Risk Score      | is equal or greater than | 50                                                                                                                       |
| Group By    |                 |                          | Source IP Address                                                                                                        |
| Time Window |                 |                          | 1 Hour                                                                                                                   |
| Title       |                 |                          | \${ruleName} for \${groupByValue1}                                                                                       |

### High Risk Alerts: ESA

The following table shows the values for the High Risk Alerts: ESA default incident rule.

| Field       | Condition Field | Condition Operator | Value                                                                                                                |
|-------------|-----------------|--------------------|----------------------------------------------------------------------------------------------------------------------|
| Name        |                 |                    | High Risk Alerts: ESA                                                                                                |
| Description |                 |                    | This incident rule captures alerts generated by the RSA ESA platform as having a Risk Score of "High" or "Critical". |
| Group:      |                 |                    | All of these                                                                                                         |
| Conditions: | Source          | is equal to        | Event Stream Analysis                                                                                                |

| Field       | Condition Field | Condition Operator       | Value                              |
|-------------|-----------------|--------------------------|------------------------------------|
|             | Risk Score      | is equal or greater than | 50                                 |
| Group By    |                 |                          | Source IP Address                  |
| Time Window |                 |                          | 1 Hour                             |
| Title       |                 |                          | \${ruleName} for \${groupByValue1} |

### IP Watch List: Activity Detected

The following table shows the values for the IP Watch List: Activity Detected default incident rule.

| Field       | Condition Field        | Condition Operator | Value                                                                                                                                                                                                                                                                                  |
|-------------|------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name        |                        |                    | IP Watch List: Activity Detected                                                                                                                                                                                                                                                       |
| Description |                        |                    | This incident rule captures alerts generated by IP addresses that have been added as "Source IP Address" *and* "Destination IP Address" conditions of the rule. To add additional IP addresses to the watch list, simply add a new Source and Destination IP Address conditional pair. |
| Group:      |                        |                    | Any of these                                                                                                                                                                                                                                                                           |
| Conditions: | Source IP Address      | is equal to        | 1.1.1.1                                                                                                                                                                                                                                                                                |
|             | Destination IP Address | is equal to        | 1.1.1.1                                                                                                                                                                                                                                                                                |
|             | Source IP Address      | is equal to        | 2.2.2.2                                                                                                                                                                                                                                                                                |
|             | Destination IP Address | is equal to        | 2.2.2.2                                                                                                                                                                                                                                                                                |
| Group By    |                        |                    | Source IP Address                                                                                                                                                                                                                                                                      |
| Time Window |                        |                    | 4 Hours                                                                                                                                                                                                                                                                                |
| Title       |                        |                    | \${ruleName}                                                                                                                                                                                                                                                                           |

### User Watch List: Activity Detected

The following table shows the values for the User Watch List: Activity Detected default incident rule.

| Field       | Condition Field | Condition Operator | Value                                                                                                                                                                                                                                 |
|-------------|-----------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name        |                 |                    | User Watch List: Activity Detected                                                                                                                                                                                                    |
| Description |                 |                    | This incident rule captures alerts generated by network users whose user names have been added as a "Source UserName" condition. To add more than one Username to the watch list, simply add an additional Source Username condition. |
| Group:      |                 |                    | Any of these                                                                                                                                                                                                                          |
| Conditions: | Source Username | is equal to        | jsmith                                                                                                                                                                                                                                |
|             | Source Username | is equal to        | jdoe                                                                                                                                                                                                                                  |
| Group By    |                 |                    | Source Username                                                                                                                                                                                                                       |
| Time Window |                 |                    | 4 Hours                                                                                                                                                                                                                               |
| Title       |                 |                    | \${ruleName}                                                                                                                                                                                                                          |

### Suspicious Activity Detected: Windows Worm Propagation

The following table shows the values for the Suspicious Activity Detected: Windows Worm Propagation default incident rule.

| Field       | Condition Field | Condition Operator | Value                                                                                                      |
|-------------|-----------------|--------------------|------------------------------------------------------------------------------------------------------------|
| Name        |                 |                    | Suspicious Activity Detected: Windows Worm Propagation                                                     |
| Description |                 |                    | This incident rule captures alerts that are indicative of worm propagation activity on a Microsoft network |
| 1st Group:  |                 |                    | All of these                                                                                               |
| Condition:  | Source          | is equal to        | Event Stream Analysis                                                                                      |
| 2nd Group:  |                 |                    | Any of these                                                                                               |
| Conditions: | Alert Name      | is equal to        | Windows Worm Activity Detected Logs                                                                        |
|             | Alert Name      | is equal to        | Windows Worm Activity Detected Packets                                                                     |
| Group By    |                 |                    | Source IP Address                                                                                          |
| Time Window |                 |                    | 1 Hour                                                                                                     |
| Title       |                 |                    | \${ruleName}                                                                                               |

### Suspicious Activity Detected: Reconnaissance

The following table shows the values for the Suspicious Activity Detected: Reconnaissance default incident rule.

| Field       | Condition Field | Condition Operator | Value                                                                                                                                                                            |
|-------------|-----------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name        |                 |                    | Suspicious Activity Detected: Reconnaissance                                                                                                                                     |
| Description |                 |                    | This incident rule captures alerts that identify common ICMP host identification techniques (i.e. "ping") accompanied by connection attempts to multiple service ports on a host |
| 1st Group:  |                 |                    | All of these                                                                                                                                                                     |
| Condition:  | Source          | is equal to        | Event Stream Analysis                                                                                                                                                            |
| 2nd Group:  |                 |                    | Any of these                                                                                                                                                                     |
| Conditions: | Alert Name      | is equal to        | Port Scan Horizontal Packet                                                                                                                                                      |
|             | Alert Name      | is equal to        | Port Scan Vertical Packet                                                                                                                                                        |
|             | Alert Name      | is equal to        | Port Scan Horizontal Log                                                                                                                                                         |
|             | Alert Name      | is equal to        | Port Scan Vertical Log                                                                                                                                                           |
| Group By    |                 |                    | Source IP Address                                                                                                                                                                |
| Time Window |                 |                    | 4 Hours                                                                                                                                                                          |
| Title       |                 |                    | \${ruleName}                                                                                                                                                                     |

### Monitoring Failure: Device Not Reporting

The following table shows the values for the Monitoring Failure: Device Not Reporting default incident rule.

| Field       | Condition Field | Condition Operator | Value                                                                                                                                 |
|-------------|-----------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Name        |                 |                    | Monitoring Failure: Device Not Reporting                                                                                              |
| Description |                 |                    | This incident rule captures any instance of an alert designed to detect the absence of log traffic from a previously reporting device |

| Field       | Condition Field | Condition Operator | Value                                           |
|-------------|-----------------|--------------------|-------------------------------------------------|
| Group:      |                 |                    | All of these                                    |
| Conditions: | Source          | is equal to        | Event Stream Analysis                           |
|             | Alert Name      | is equal to        | No logs traffic from device in given time frame |
| Group By    |                 |                    | Source IP Address                               |
| Time Window |                 |                    | 2 Hours                                         |
| Title       |                 |                    | \${ruleName}                                    |

### Web Threat Detection

The following table shows the values for the Web Threat Detection default incident rule.

| Field       | Condition Field | Condition Operator | Value                                                                                  |
|-------------|-----------------|--------------------|----------------------------------------------------------------------------------------|
| Name        |                 |                    | Web Threat Detection                                                                   |
| Description |                 |                    | This incident rule captures alerts generated by the RSA Web Threat Detection platform. |
| Group:      |                 |                    | All of these                                                                           |
| Condition:  | Source          | is equal to        | Web Threat Detection                                                                   |
| Group By    |                 |                    | Alert Rule Id                                                                          |
| Time Window |                 |                    | 1 Hour                                                                                 |
| Title       |                 |                    | \${ruleName} for \${groupByValue1}                                                     |

### User Entity Behavior Analytics

The following table shows the values for the User Entity Behavior Analytics default incident rule.

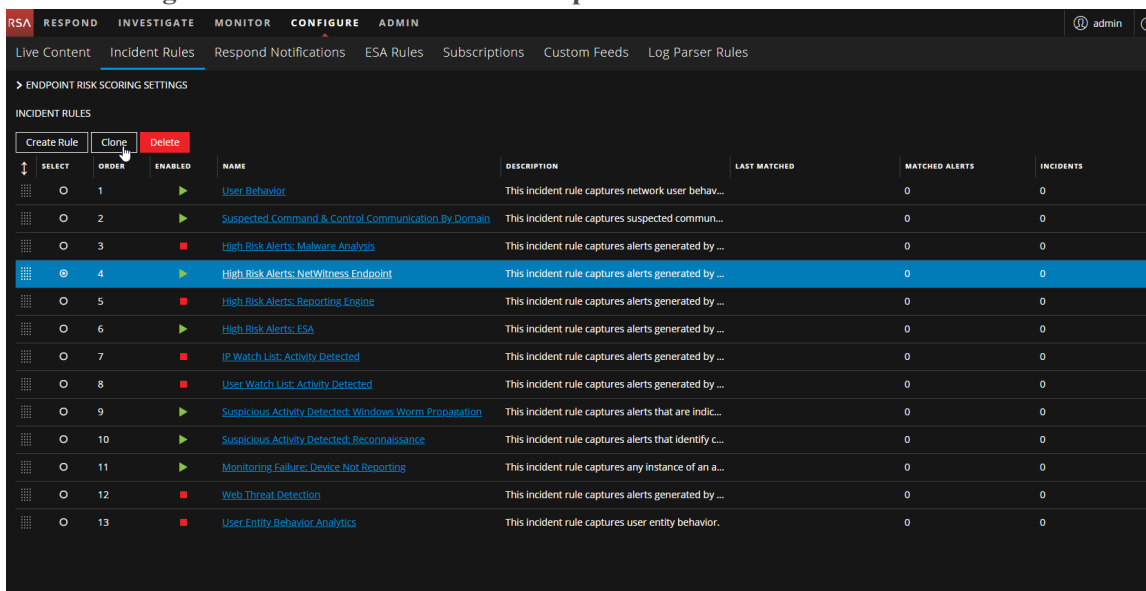
| Field       | Condition Field | Condition Operator | Value                                             |
|-------------|-----------------|--------------------|---------------------------------------------------|
| Name        |                 |                    | User Entity Behavior Analytics                    |
| Description |                 |                    | This incident rule captures user entity behavior. |
| Group:      |                 |                    | All of these                                      |

| Field       | Condition Field | Condition Operator | Value                              |
|-------------|-----------------|--------------------|------------------------------------|
| Condition:  | Source          | is equal to        | User Entity Behavior Analytics     |
| Group By    |                 |                    | Classifier id                      |
| Time Window |                 |                    | 1 Hour                             |
| Title       |                 |                    | \${ruleName} for \${groupByValue1} |

## Create a NetWitness Endpoint Incident Rule using File Hash

To aggregate NetWitness Endpoint alerts based on the File Hash, create another NetWitness Endpoint Rule using the File Hash as the Group By value. To do this, you clone the default NetWitness Endpoint incident rule and change the Group By value.

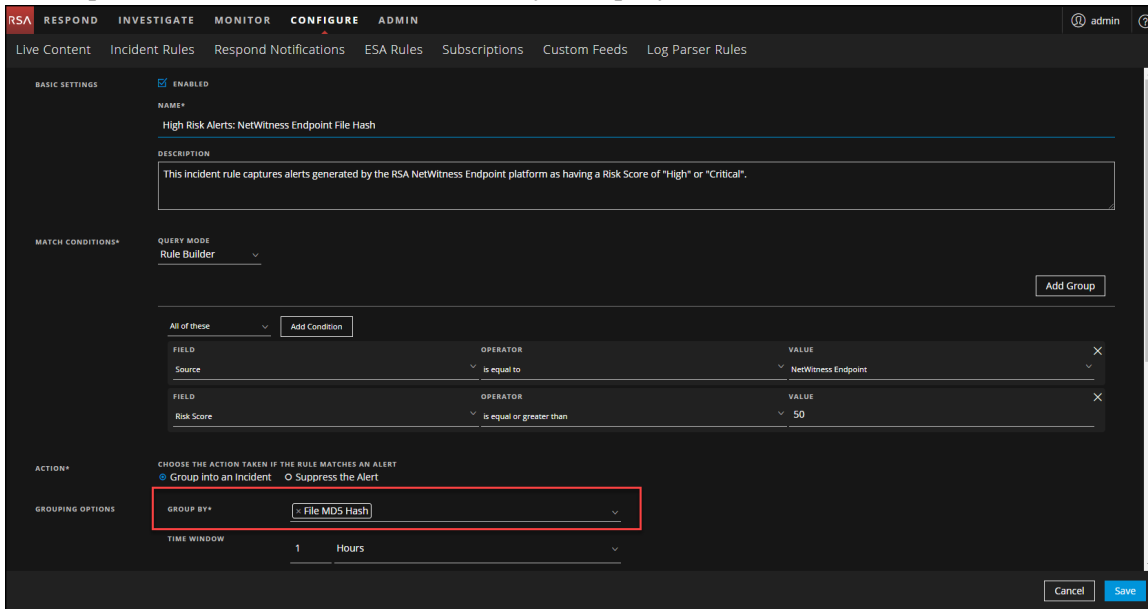
1. Go to **CONFIGURE > Incident Rules**.  
The Incident Rules view is displayed.
2. Select the **High Risk Alerts: NetWitness Endpoint** default incident rule and click **Clone**.



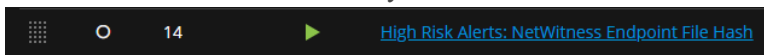
You will receive a message that you successfully cloned the selected rule.

3. Change the **Name** of the rule to an appropriate name, such as High Risk Alerts: NetWitness Endpoint File Hash.

- In the **Group By** field, remove the previous Group By value and add **File MD5 Hash**. It is important that File MD5 Hash is the only Group By value listed.



- If you are ready to enable your rule, in the Basic Settings section, select **Enabled**.
- Click **Save** to create the rule. The Incident Rules view shows your new rule.



- Verify the order of your incident rules. For more information, see [Verify the Order of Your Incident Rules](#).



## Configure Risk Scoring Settings for Automated Incident Creation

**Note:** The information in this topic applies to RSA NetWitness® Platform Version 11.3 and later.

Endpoint Risk Scoring Settings only apply to NetWitness Endpoint.

In addition to automatically creating incidents with predefined rules and rules that you define, NetWitness Respond automatically creates risk scoring incidents for suspicious files and hosts when defined risk score thresholds are crossed. In the background, it monitors the following types of alerts and calculates risk scores for each file and host:

- Critical and High priority alerts from NetWitness Respond
- Medium priority Endpoint alerts from ESA

NetWitness Respond calculates risk score using a combination of the number of distinct alerts and the severity of alerts associated with the file or host. A higher risk score indicates more of these types of alerts. When the calculated risk score exceeds the specified threshold, NetWitness Respond does one of the following during the specified time window, such as 1 day:

- Creates a risk scoring alert and uses it to create a risk scoring incident
- Adds risk scoring alerts along with associated events to the same incident

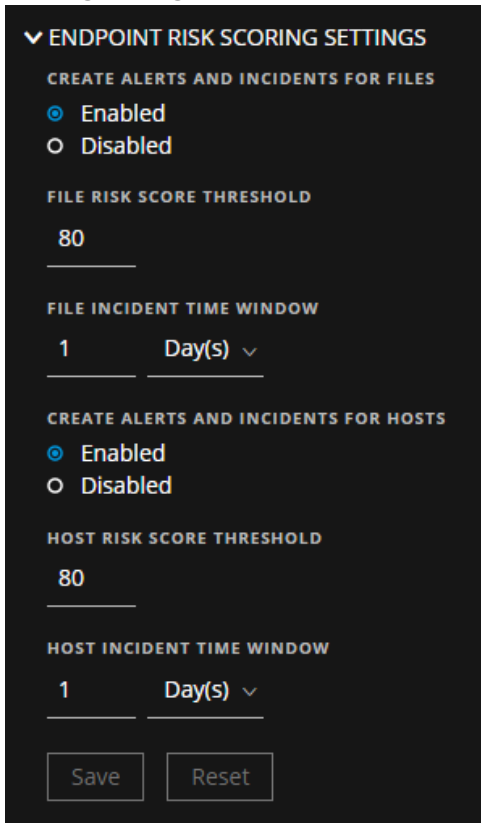
For more information on configuring NetWitness Endpoint, see the *NetWitness Endpoint Configuration Guide*.

### To configure the Endpoint Risk Scoring Settings:

You should leave the Endpoint Risk Scoring Settings at the default values. However, if you are getting too many risk scoring alerts and incidents created, increase the risk score threshold to a higher value. Also, if you are getting too many incidents created for the same hosts or files, increase the time window to add more alerts to the same risk scoring incidents. If you are not seeing many risk scoring incidents, you can either decrease the risk scoring thresholds for hosts and files or decrease the incident time windows.

1. Go to **CONFIGURE > Incident Rules**.  
The Incident Rules view is displayed.

- Click the arrow in front of **ENDPOINT RISK SCORING SETTINGS** to expand the Endpoint Risk Scoring Settings section.



The screenshot shows a dark-themed configuration panel for 'ENDPOINT RISK SCORING SETTINGS'. It is expanded, showing a dropdown arrow on the left. The panel is divided into two main sections: 'CREATE ALERTS AND INCIDENTS FOR FILES' and 'CREATE ALERTS AND INCIDENTS FOR HOSTS'. Each section has a radio button for 'Enabled' (selected) and 'Disabled'. Below each section are input fields for 'FILE RISK SCORE THRESHOLD' and 'HOST RISK SCORE THRESHOLD', both set to '80'. There are also input fields for 'FILE INCIDENT TIME WINDOW' and 'HOST INCIDENT TIME WINDOW', both set to '1' with a 'Day(s)' dropdown menu. At the bottom, there are 'Save' and 'Reset' buttons.

- In the Endpoint Risk Scoring Settings section, adjust the settings as follows:
  - Create Alerts and Incidents for Files:**
    - Select **Enabled** to automatically create risk scoring alerts and incidents for suspicious files. When calculated file risk scores go above the file risk score threshold, it triggers the creation of risk scoring alerts and incidents.
    - Select **Disabled** to stop automatically creating risk scoring alerts and incidents. If you disable it, incidents are not created for suspicious files where risk scores are high.
  - File Risk Score Threshold:** The File Risk Score Threshold is the risk score level used to trigger alert and incident creation. The File Risk Score Threshold range is from 0-100. For example, if the File Risk Score Threshold is 80 and the calculated risk score of a suspicious Openme.rar file is 81, which is over the Risk Score Threshold of 80, NetWitness Respond creates a risk scoring alert and incident or adds a risk scoring alert to an existing incident depending on the file incident time window.
    - If you are seeing too many alerts and incidents, increase the risk score threshold.
    - If you are not seeing many alerts and incidents, decrease the risk score threshold.
  - File Incident Time Window:** The File Incident Time Window is the period of time to wait before creating another incident. The file incident time window range is from 1-24 (hours or days). For example, the suspicious Openme.rar file has a calculated risk score of 81 and a file

time window of 1 day. A risk scoring alert and incident is created for the Openme.rar file. During the time window, any similar risk scoring alerts with the same name created for the Openme.rar file get added to the same incident. At the end of the time window (day 1), if the calculated risk score of the file is still over the file risk score threshold and a change occurs with the risk score, another risk scoring alert and incident gets created and any new risk scoring alerts associated with the file get added to the new incident until the next time window (day 3).

- If you are seeing too many alerts and incidents, increase the incident time window.
- If you are not seeing many alerts and incidents, decrease the incident time window.

d. **Create Alerts and Incidents for Hosts:**

- Select **Enabled** to automatically create risk scoring alerts and incidents for suspicious hosts. When calculated host risk scores go above the host risk score threshold, it triggers the creation of risk scoring alerts and incidents.
- Select **Disabled** to stop automatically creating risk scoring alerts and incidents when calculated host risk scores go above the host risk score threshold. If you disable it, incidents are not created for suspicious hosts where risk scores are high.

e. **Host Risk Score Threshold:** The Host Risk Score Threshold is the risk score level used to trigger alert and incident creation. The host risk score threshold range is from 0-100. For example, if the Host Risk Score Threshold is 80 and the calculated risk score of a suspicious host IP address is 81, which is over the Risk Score Threshold of 80, NetWitness Respond creates a risk scoring alert and incident or adds a risk scoring alert to an existing incident depending on the file incident time window.

- If you are seeing too many alerts and incidents, increase the risk score threshold.
- If you are not seeing many alerts and incidents, decrease the risk score threshold.

f. **Host Incident Time Window:** The Host Incident Time Window is the period of time to wait before creating another incident. The host incident time window range is from 1-24 (hours or days). For example, the suspicious host has a calculated risk score of 81 and a Host Time Window of 1 day. During the time window, any similar risk scoring alerts with the same name created for the suspicious host get added to the same incident. At the end of the time window (day 1), if the calculated risk score of the host is still over the host risk score threshold and a change occurs with the risk score, another risk scoring alert and incident gets created. Any new risk scoring alerts associated with that suspicious host add to that incident until the next time window.

- If you are seeing too many risk scoring alerts and incidents, increase the incident time window.
- If you are not seeing many risk scoring alerts and incidents, decrease the incident time window.

4. Click **Save**.

## Configure Respond Email Notification Settings

NetWitness Respond notification settings enable email notifications to be sent to SOC Managers and the Analyst assigned to an incident when an incident is created or updated.

1. Go to **CONFIGURE > Respond Notifications**.


The Respond Notifications Settings view is displayed.

The screenshot shows the 'Respond Notification Settings' page in the NetWitness Respond interface. The page is divided into several sections:

- EMAIL SERVER:** A dropdown menu currently showing 'Respond Notification Server'. A link for 'Email Server Settings' is provided below.
- SOC Manager Email Addresses:** A list of four email addresses: socmanager1@email.com, socmanager2@email.com, socmanager3@email.com, and socmanager4@email.com. Each address has a small square icon with a minus sign to its right for removal. Below the list is a text input field labeled 'Enter an email address to add' and an 'Add' button.
- Notification Types:** A table with columns for 'TYPE', 'SEND TO ASSIGNEE', and 'SEND TO SOC MANAGERS'.
 

| TYPE             | SEND TO ASSIGNEE                    | SEND TO SOC MANAGERS                |
|------------------|-------------------------------------|-------------------------------------|
| Incident Updated | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Incident Created | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |

At the bottom of the page, a yellow warning message reads: '▲ You have unsaved changes. Click Apply to save.' and a blue 'Apply' button is located in the bottom right corner.

2. In the **Email Server** section, select the email server from the drop-down list that will send out email notifications when the notification settings are enabled.  
If there is no email server configured, you do not see an email server listed in the drop-down list. You have to configure an email server before you can continue with this procedure. To configure an email server, click the **Email Server Settings** link. For more information, click the help icon or refer to the *System Configuration Guide*.
3. In the **SOC Manager Email Addresses** section, add the email addresses of the SOC Managers that you want to receive email notifications. To add an SOC Manager email address to the list, type it in the field that shows **Enter an email address to add** and click **Add**. To remove an SOC Manager email address from the list, click  next to the email address to be removed.
4. In the **Notification Types** section, select who should receive an email notification when an incident is created and when an incident is updated.
  - **Send to Assignee:** An email is sent to the Analyst assigned to the incident.
  - **Send to SOC Manager:** An email is sent to all of the addresses listed in the **SOC Manager Email Addresses** list.
5. Click **Apply**. Changes take effect immediately.

**Note:** If user email address information is updated in the ADMIN > Security > Users tab, it can take up to two minutes for the new email changes to take effect. Any incident creation or incident update email notifications sent during this time go to the old email address.

### Migration Considerations

Notification Settings do not migrate from NetWitness Platform version 10.6.x to 11.1 and later. The Incident Management Notification Settings in 10.6.x are different from the Respond notification settings available in 11.1 and later. You will need to manually update the Respond Notification Settings in version 11.1 and later.

Notification Servers from 10.6.x are not displayed in the Email Server drop-down list. The email servers settings must be added to the Global Notification Servers (ADMIN > System > Global Notifications > Server tab).

Custom Incident Management notification templates cannot be migrated to 11.1 and later. No custom templates are supported in 11.1 and later.

## 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 NetWitness Respond 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 NetWitness Respond 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
- Tasks
- Journal entries

Logs track retention and manual deletion so you can see what has been deleted. You can view Respond Server logs in the following locations:

- **Respond Server Service log:** `/var/log/netwitness/respond-server/respond-server.log`
- **Respond Server Audit log:** `/var/log/netwitness/respond-server/respond-server.audit.log`

The data retention period that you set here does not apply to Archer or other third-party SOC tools. Alerts and incidents from other systems must be deleted separately.

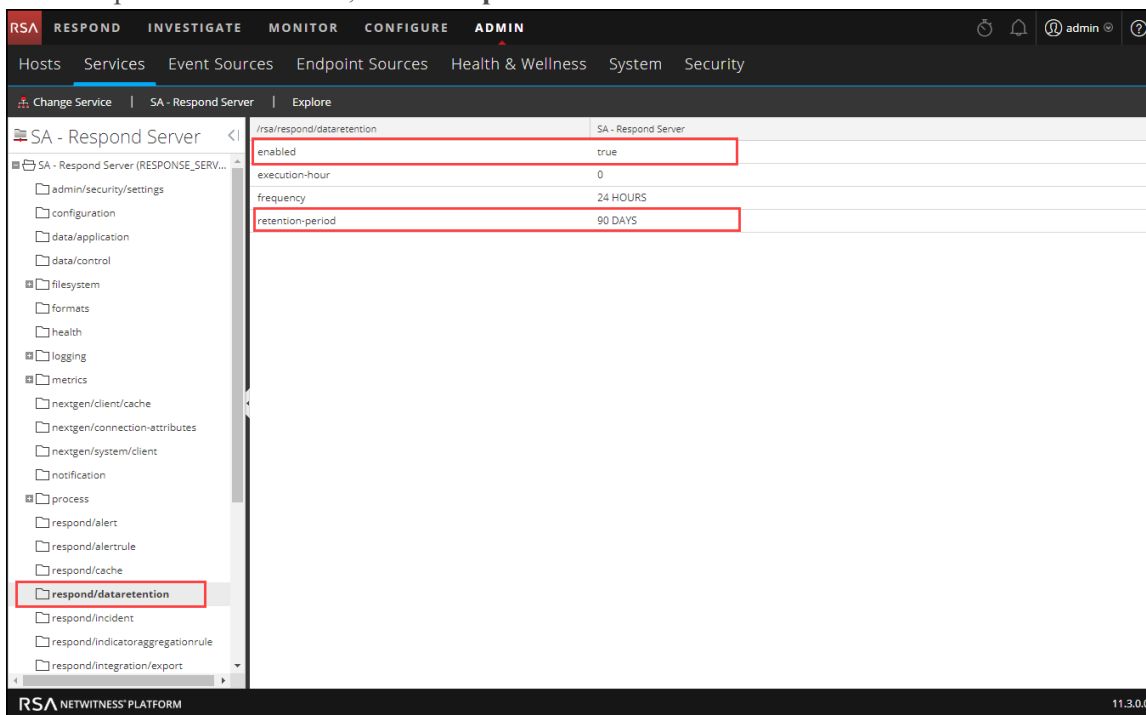
### Prerequisites

The Administrator role must be assigned to you.

### Procedure

1. Go to **ADMIN > Services**, select the Respond Server service, and then select   > **View > Explore**.

- In the Explore view node list, select **respond/dataretention**.



- In the **enabled** field, select **true** to delete incidents and alerts older than the retention period. The scheduler runs every 24 hours at 23:00. You will see a notice that the configuration was successfully updated.
- In the **retention-period** field, type the number of days to retain incidents and alerts. For example, type 30 DAYS, 60 DAYS, 90 DAYS, 120 DAYS, 365 DAYS, or any number of days. A message informs you that the configuration was successfully updated.

## Result

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

## Set a Retention Period for Risk Scoring Data



This allows you to retain risk score data for a certain period of time and then delete it. A shorter retention period frees up disk space sooner.

Data retention for risk score is enabled by default with retention period configured for 30 days. You can also reconfigure the retention period. Data deleted after the retention period cannot be recovered.

### Prerequisites

The Administrator role must be assigned to you.

### Procedure

1. Go to **ADMIN > Services**, select the Respond Server service, and then select   > **View > Explore**.
2. In the Explore view node list, select **respond/risk/data/retention**.
3. In the **retention-period** field, enter the number of days to retain risk score related events. For example, 20 DAYS. The default and maximum retention-period is 30 days. You will see a notice that the configuration is successfully updated.
4. In the **Frequency** field, enter the frequency to run the retention in days. The default frequency is 1 day. You will see a notice that the configuration is successfully updated.
5. Restart respond server for changes to take effect.

**Note:** Data retention starts after every respond server restart.

### Result

After the retention period ends, the scheduler permanently deletes all the risk score alert context older than the specified period.



## 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:

- NetWitness Platform 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 NetWitness Respond. 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 NetWitness Respond, 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:  
`/var/lib/netwitness/respond-server/scripts/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 figure, a hashed value displays for the destination IP address in the Event Details:

| User        |        |             |                                                                |
|-------------|--------|-------------|----------------------------------------------------------------|
| Destination | Device | Port        | 4369                                                           |
|             |        | MAC Address | 00:00:00:00:00:00                                              |
|             |        | IP Address  | 81B7DC4A84D441BFAED06E3D46A19C49D17B4157FBECDEE868FD7D21A27F77 |
|             |        | Geolocation |                                                                |

New alerts will display obfuscated data.

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

## Manage Incidents in Archer Cyber Incident & Breach Response

If you want to manage incidents in RSA Archer® Cyber Incident & Breach Response instead of NetWitness Respond, you have to configure system integration settings in the Respond Server service Explore view. After you configure the system integration settings, all incidents are managed in Archer Cyber Incident & Breach Response. Incidents created before the integration will not be managed in Archer Cyber Incident & Breach Response.

**Caution:** If you are managing incidents in Archer Cyber Incident & Breach Response instead of NetWitness Respond, do not use the following in the Respond view: Incidents List view, Incident Details view, and Tasks List view. Do not create incidents from the Respond Alerts List view or from Investigate.



For more detailed integration information, see the *RSA Archer Integration Guide*.

### Prerequisites

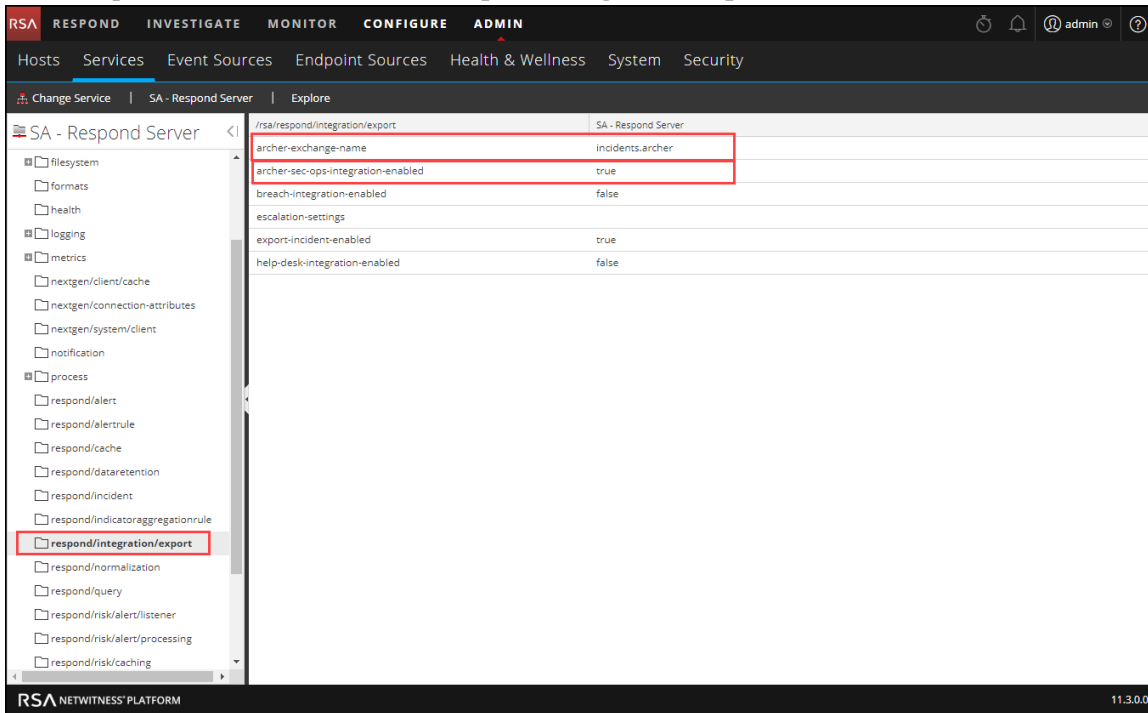
- Archer Cyber Incident & Breach Response 1.3.1.2 (NetWitness Platform 11.0 works only with Archer Cyber Incident & Breach Response 1.3.1.2.)

### Procedure

Follow this procedure to configure Respond Server service settings to manage incidents in Archer Cyber Incident & Breach Response.

1. Go to **ADMIN > Services**, select the Respond Server service, and then select   > **Config** > **Explore**.

2. In the Explore view node list, select **respond/integration/export**.



3. In the **archer-exchange-name** field, type `incidents.archer`.  
You will see a notice that the configuration was successfully updated.
4. In the **archer-sec-ops-integration-enabled** field, select **true**.  
A message informs you that the configuration was successfully updated.  
Incidents will be managed exclusively in Archer Cyber Incident & Breach Response.




## Configure the Option to Send Incidents to RSA Archer

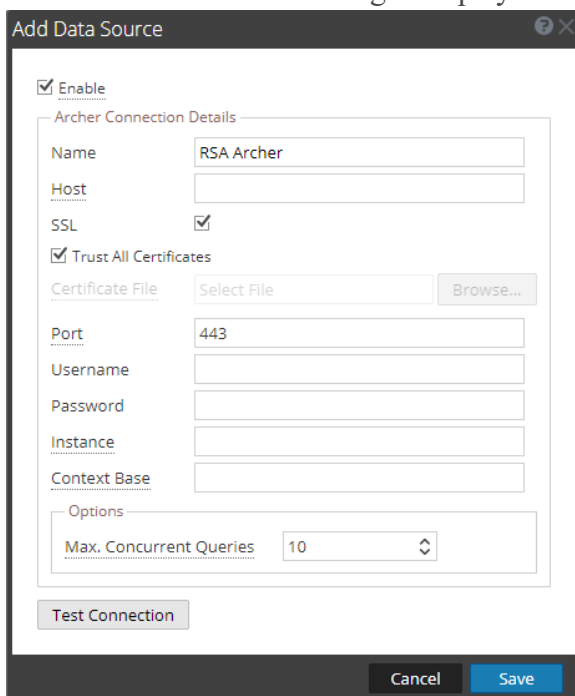
**Note:** The information in this topic applies to RSA NetWitness® Platform Version 11.2 and later.

If you want to manage incidents in NetWitness Respond, you have the option to configure the NetWitness Platform so that you can send incidents to RSA Archer® Cyber Incident & Breach Response. If RSA Archer is configured as a data source in Context Hub, you can send incidents to Archer Cyber Incident & Breach Response and you will be able to see a Send to Archer option and a Sent to Archer status in NetWitness Respond. For information on how to use the Send to Archer option and Sent to Archer status, see the *NetWitness Respond User Guide*.

### Add RSA Archer as a Data Source for Context Hub

To configure sending incidents to Archer Cyber Incident & Breach Response from NetWitness Respond, RSA Archer must be configured as a data source for Context Hub. For more detailed instructions for configuring the RSA Archer data source, see the "Configure Archer as Data Source" topic in the *Context Hub Configuration Guide*.

1. Go to **ADMIN > Services**.  
The Services view is displayed.
2. Select the Context Hub service, and then select   > **View > Config**.  
The Services Config view is displayed.
3. On the **Data Sources** tab, click  > **RSA Archer**.  
The **Add Data Source** dialog is displayed.



4. Provide the following information:

- By default, the **Enable** checkbox is selected. If this option is unchecked, the save button is disabled, you cannot add the data source, and cannot view the contextual information.
- Enter the following fields:
  - **Name:** Enter a name for Archer data source.
  - **Host:** Enter the hostname or IP address where Archer server is installed.
  - **SSL:** By default this option is selected and enables SSL communication to Archer .
  - **Trust All Certificates:** Select this checkbox to add the data source without validating the certificate. If you uncheck this option, you need to upload a valid Endpoint server certificate for the connection to be successful.
  - **Port:** The default port is 443.
  - **Username:** Enter the Archer Server username.
  - **Password:** Enter the Archer Server password.
  - **Instance:** Enter the Instance name from which you want to extract data. An RSA Archer instance is a single setup that includes unique content in a database, the connection to the database, the interface, and login. You might have individual instances for each office location or region or for development, test, and production environments. The Instance Database stores the RSA Archer content for a specific instance.
  - **Context Base:** Enter the virtual directory name where the files are stored. For example, rsaarcher located at the RSA Archer web address <https://archer.company.com/rsaarcher/default.aspx>. If the files are stored in the IIS default web address <https://archer.company.com/default.aspx>, then this field must be empty.
  - **Max. Concurrent Queries:** You can configure the maximum number of concurrent queries defined by the Context Hub service to be run against the configured data sources. The default value is 10.
- 5. Click **Test Connection** to test the connection between Context Hub and the Archer data source.
- 6. Click **Save**.

RSA Archer is added as a data source for Context Hub and is displayed in the **Data Sources** tab. A Send to Archer button and Sent to Archer status is visible in NetWitness Respond.

## Configure Threat Aware Authentication

**Note:** The information in this topic applies to RSA NetWitness® Platform Version 11.3 and later.

NetWitness Platform creates a list of suspicious users that have an incident created against them and sends it to RSA SecurID Access. The list contains the email IDs of the corresponding suspicious users associated with the incident. RSA SecurID Access maintains this high-risk users list and reduces the access levels or blocks such users using defined policies. When an incident is closed in RSA NetWitness Platform, the associated email IDs are automatically removed from the RSA SecurID high-risk user list.

By default this configuration is disabled in the NetWitness Server. You can enable this feature by editing the yml file located at `/etc/netwitness/respond-server/respond-server.yml`.

### Enable Threat Aware Authentication

To enable this configuration:

1. Create a yml file at `/etc/netwitness/respond-server/respond-server.yml`
2. Edit and enter `rsa.respond.securid-integration.enabled: true`
3. Enter `rsa.security.pki.use-jvm-trust: true` to enable the configuration.

```
[root@adminserver ~]# vi /etc/netwitness/respond-server/respond-server.yml
[root@adminserver ~]# cat /etc/netwitness/respond-server/respond-server.yml
rsa.respond.securid-integration.enabled: true
rsa.security.pki.use-jvm-trust: true
[root@adminserver ~]# service rsa-nw-respond-server restart
Redirecting to /bin/systemctl restart rsa-nw-respond-server.service
[root@adminserver ~]#
```

4. Save the yml file and restart the Respond Server service.

**Note:** Make sure you perform the above configuration if you have enabled a stand-by NW server. In case the primary NW server fails and goes offline, this configuration will allow the standby NW server to connect to RSA SecurID.

### Obtain SecurID API Key

A super administrator must generate and download a SecurID API key, and connect to RSA SecurID Access.

To obtain the API key from RSA SecurID Access:

1. Log in to the **RSA SecurID Access Cloud Administration** Console.
2. Click **Platform > API Key Management**.
3. Click **ADD**.  
The new key is displayed.
4. Change the **Administrator** role to **Super Administrator**.
5. Click **Save** and **Download** to download and save the API key file.

For more information about generating the API Keys and other related details, see "Manage the Cloud Administration API Keys" at <https://community.rsa.com/docs/DOC-94440> and "Determining Access Requirements for High-Risk Users in the Cloud Authentication Service" topic at <https://community.rsa.com/docs/DOC-90586>.

### Configure RSA SecurID Access API Key

To configure RSA SecurID Access API key using RSA NetWitness Shell:

1. SSH to the NetWitness Server.
2. Type the command `nw-shell`.  
A console window is displayed.



```
[root@adminserver ~]# nw-shell
RSA Netwitness Shell. Version: 4.9.0-SNAPSHOT
offline » connect --service respond-server
```

3. Type `connect --service respond-server.<service-id>` to connect to the Respond Server. For example: `connect --service respond-server.36334277-9f93-4402-9523-ed15ad543bfa`.  
You can obtain the `<service_id>` from `cat /etc/netwitness/respond-server/service-id`.
1. Type `login` and enter admin username and password.
2. To set the API key:
  - a. Navigate to set-api-key node: `cd /rsa/respond/securid/set-api-key`
  - b. type: `invoke --file <path to api key>`

**Note:** The path to the API key is the location on the NetWitness Server.

3. Test the connection using the command:
  - a. `cd /rsa/respond/securid/test-secur-id-connection`
  - b. Type `invoke`.  
A "Connection OK" message is displayed if test connection is successful.





4. To start the process use the command:
  - a. `cd /rsa/respond/securid/process-incidents`
  - b. `invoke.`

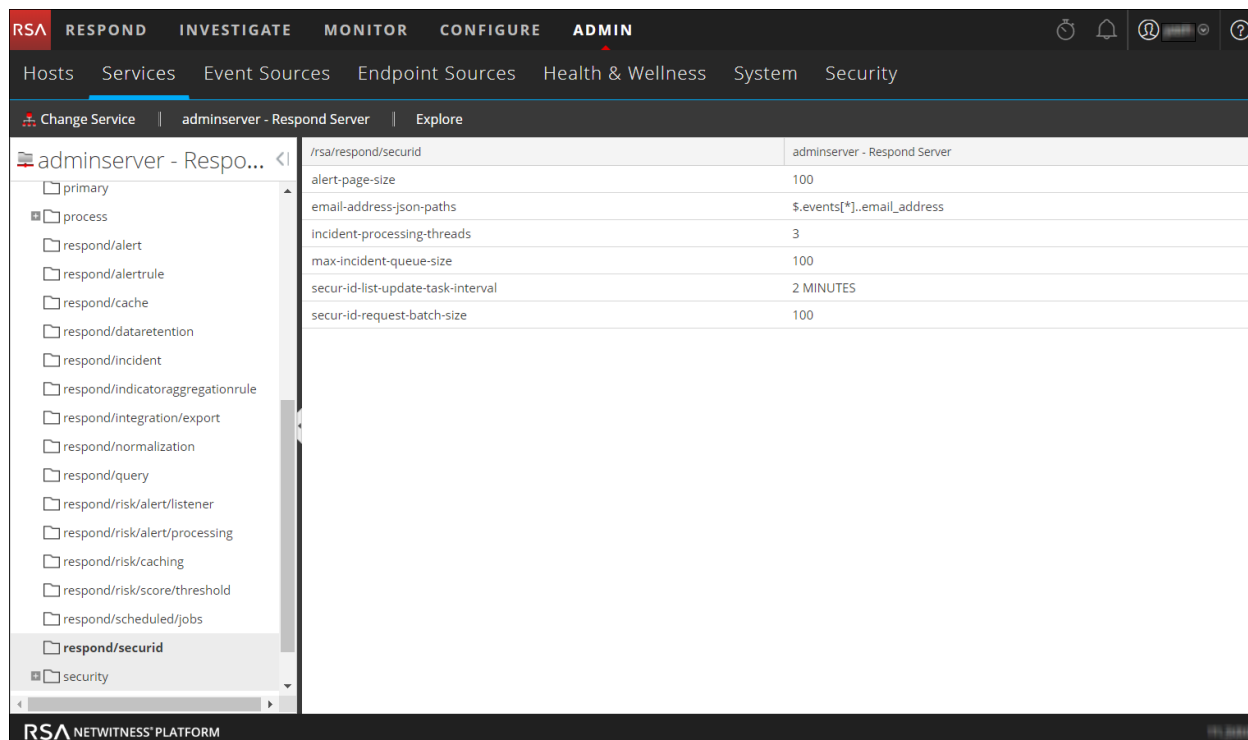
For more information on how to define policies, see the *RSA SecurID Access Guide* on RSA link.

### Configure Sync Frequency

By default, the sync frequency is set to 15 minutes.

To edit the frequency:

1. Log in to NetWitness Platform.
2. Go to **ADMIN > Services**, select the Respond Server service, and then select   > **View > Explore**.
3. Edit the duration at `rsa/respond/securid`.



| Path                               | Value                        |
|------------------------------------|------------------------------|
| /rsa/respond/securid               | adminserver - Respond Server |
| alert-page-size                    | 100                          |
| email-address-json-paths           | \$.events[*].email_address   |
| incident-processing-threads        | 3                            |
| max-incident-queue-size            | 100                          |
| secur-id-list-update-task-interval | 2 MINUTES                    |
| secur-id-request-batch-size        | 100                          |

## 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 Incident Rules view displays these counts in columns on the right.

| SELECT                           | ORDER | ENABLED | NAME                                                   | DESCRIPTION                                           | LAST MATCHED           | MATCHED ALERTS | INCIDENTS |
|----------------------------------|-------|---------|--------------------------------------------------------|-------------------------------------------------------|------------------------|----------------|-----------|
| <input type="radio"/>            | 1     |         | User Behavior                                          | This incident rule captures network user behav...     |                        | 0              | 0         |
| <input type="radio"/>            | 2     |         | Suspected Command & Control Communication By Domain    | This incident rule captures suspected communi...      |                        | 0              | 0         |
| <input type="radio"/>            | 3     |         | High Risk Alerts: Malware Analysis                     | This incident rule captures alerts generated by ...   |                        | 0              | 0         |
| <input type="radio"/>            | 4     |         | High Risk Alerts: NetWitness Endpoint                  | This incident rule captures alerts generated by ...   | 02/01/2019 08:48:30 pm | 664            | 249       |
| <input type="radio"/>            | 5     |         | High Risk Alerts: Reporting Engine                     | This incident rule captures alerts generated by ...   |                        | 0              | 0         |
| <input type="radio"/>            | 6     |         | High Risk Alerts: ESA                                  | This incident rule captures alerts generated by ...   | 02/01/2019 12:50:55 pm | 53             | 1         |
| <input type="radio"/>            | 7     |         | IP Watch List: Activity Detected                       | This incident rule captures alerts generated by ...   |                        | 0              | 0         |
| <input type="radio"/>            | 8     |         | User Watch List: Activity Detected                     | This incident rule captures alerts generated by ...   |                        | 0              | 0         |
| <input type="radio"/>            | 9     |         | Suspicious Activity Detected: Windows Worm Propagation | This incident rule captures alerts that are indic...  |                        | 0              | 0         |
| <input type="radio"/>            | 10    |         | Suspicious Activity Detected: Reconnaissance           | This incident rule captures alerts that identify c... |                        | 0              | 0         |
| <input type="radio"/>            | 11    |         | Monitoring Failure: Device Not Reporting               | This incident rule captures any instance of an a...   |                        | 0              | 0         |
| <input type="radio"/>            | 12    |         | Web Threat Detection                                   | This incident rule captures alerts generated by ...   |                        | 0              | 0         |
| <input checked="" type="radio"/> | 13    |         | User Entity Behavior Analytics                         | This incident rule captures user entity behavior.     | 02/01/2019 09:01:06 pm | 2729           | 1393      |
| <input type="radio"/>            | 14    |         | High Risk Alerts: NetWitness Endpoint Detector IP      | This incident rule captures alerts generated by ...   |                        | 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.

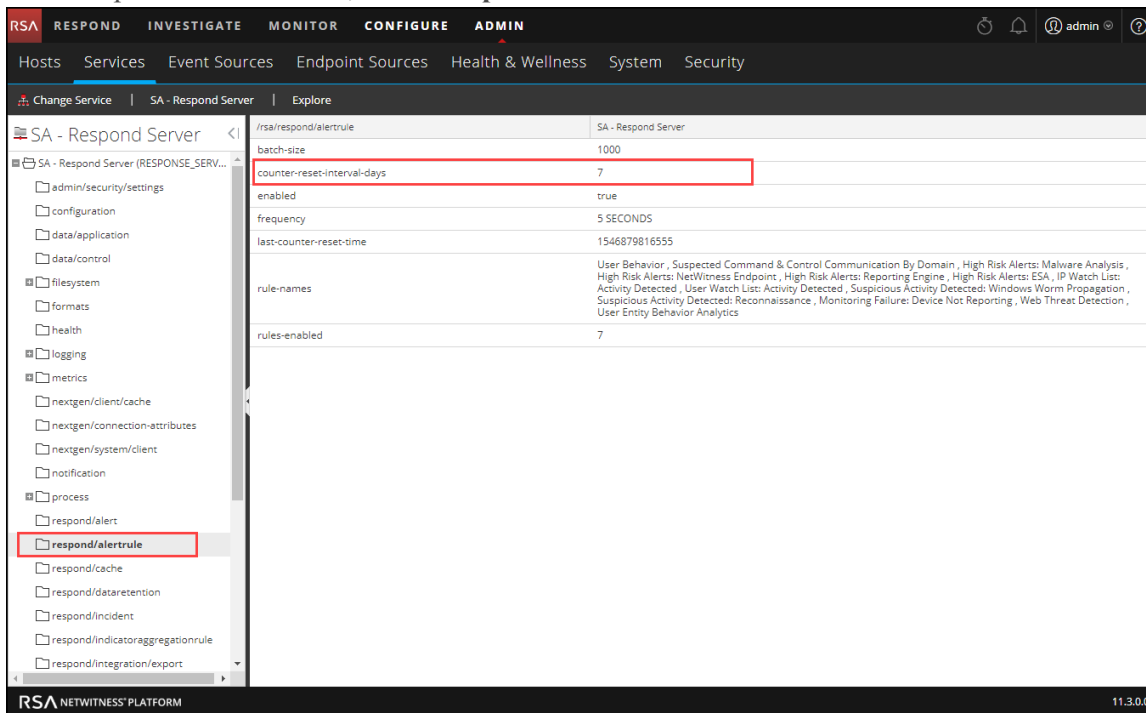
By default, these values reset to zero every 7 days. Depending on how long you want the counts to continue, you can change the default number of days.


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

### To set a counter for matched alerts and incidents:

1. Go to **ADMIN > Services**, select the Respond Server service and then select   > **View > Explore**.

- In the Explore view node list, select **respond/alertrule**.



- In the right panel, type the number of days in the **counter-reset-interval-days** field.
- Restart the Respond Server service for the new setting to take effect. To do this, go to **ADMIN > Services**, select the Respond Server service, and then select  > **Restart**.

## Configure a Database for the Respond Server Service



This procedure is required only if you need to change the database configuration for Respond Server after the deployment of the NetWitness or ESA Primary hosts and their corresponding services. You have to select the ESA Primary server to act as the database host for NetWitness Respond application data, such as alerts, incidents, and tasks. You also have to select the NetWitness Server to act as the database host for NetWitness Respond control data, such as incident rules and categories.

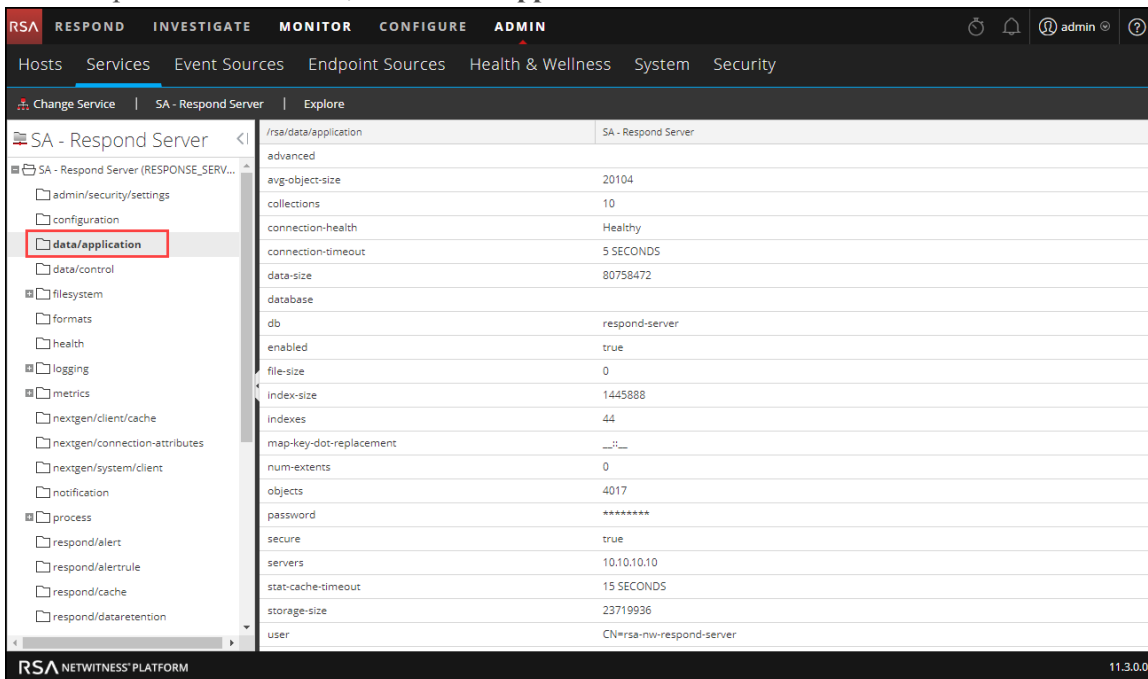
### Prerequisites

Ensure that:

- The Respond Server service is installed and running on NetWitness Platform.
- An ESA host is installed and configured.

### Procedure

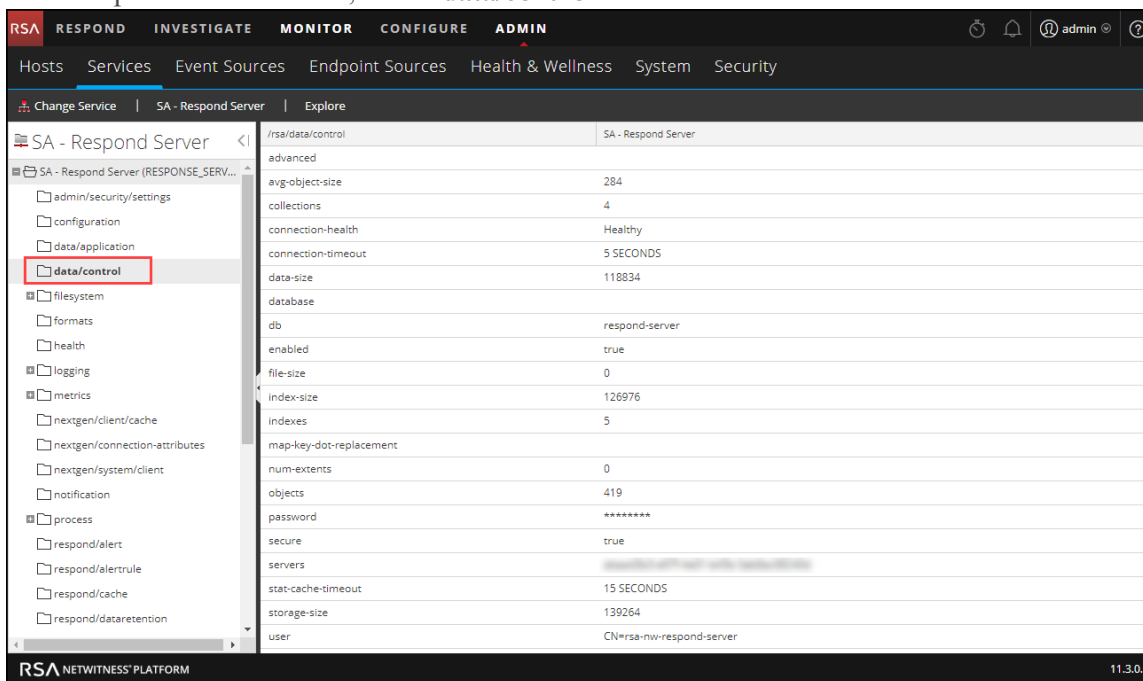
1. Go to **ADMIN > Services**.  
The Services view is displayed.
2. In the Services panel, select the **Respond Server** service and then select   > **View > Explore**.
3. In the Explore view node list, select **data/application**.



4. Provide the following information:


- **db:** The database name. The default value is respond-server.
- **password:** The password used for the deployment of the ESA primary server (password for deploy\_admin user).
- **servers:** The hostname or IP address of the **ESA primary server** to act as the database host for NetWitness Respond application data, such as alerts, incidents, and tasks.
- **user:** Enter **deploy\_admin**.

5. In the Explore view node list, select **data/control**.



6. Provide the following information:

- **db:** The database name. The default value is respond-server.
- **password:** The password used for the deployment of the NetWitness Server (password for deploy\_admin user).
- **servers:** The hostname or IP address of the **NetWitness Server** to act as the database host for NetWitness Respond control data, such as incident rules and categories.
- **user:** Enter **deploy\_admin**.

7. Restart the Respond Server service. To do this, go to **ADMIN > Services**, select the Respond Server service, and then select  > **Restart**.

**Note:** Restarting the Respond Server service is required for the database configuration to be complete.

## NetWitness Respond Configuration Reference

---

This section contains reference information for configuring NetWitness Respond.

### Configure View

The Configure view enables you to configure NetWitness Respond functionality.

You can configure incident rules to automate the Respond workflow for automatically creating incidents. You can also configure notification settings to send emails when incidents are created or updated.

#### Topics

- [Incident Rules View](#)
- [Incident Rule Details View](#)
- [Respond Notification Settings View](#)
- [Aggregation Rules Tab](#)
- [New Rule Tab](#)

## Incident Rules View

The Incident Rules view enables you to manage the automated incident creation process. NetWitness Respond creates incidents in two ways:

- **Incident Rules:** NetWitness Platform provides preconfigured rules that you can adjust for your environment. You can also create your own rules.
- **Risk Scoring:** (Endpoint Risk Scoring Settings are available in NetWitness Platform version 11.3 and later and only apply to NetWitness Endpoint.) NetWitness Respond uses these settings to automatically create risk scoring incidents for suspicious files and hosts that cross the defined risk score thresholds. If you get too many or too few risk scoring incidents, you can adjust these thresholds.

**Note:** The information in this topic applies to RSA NetWitness® Platform 11.1 and later.

### What do you want to do?

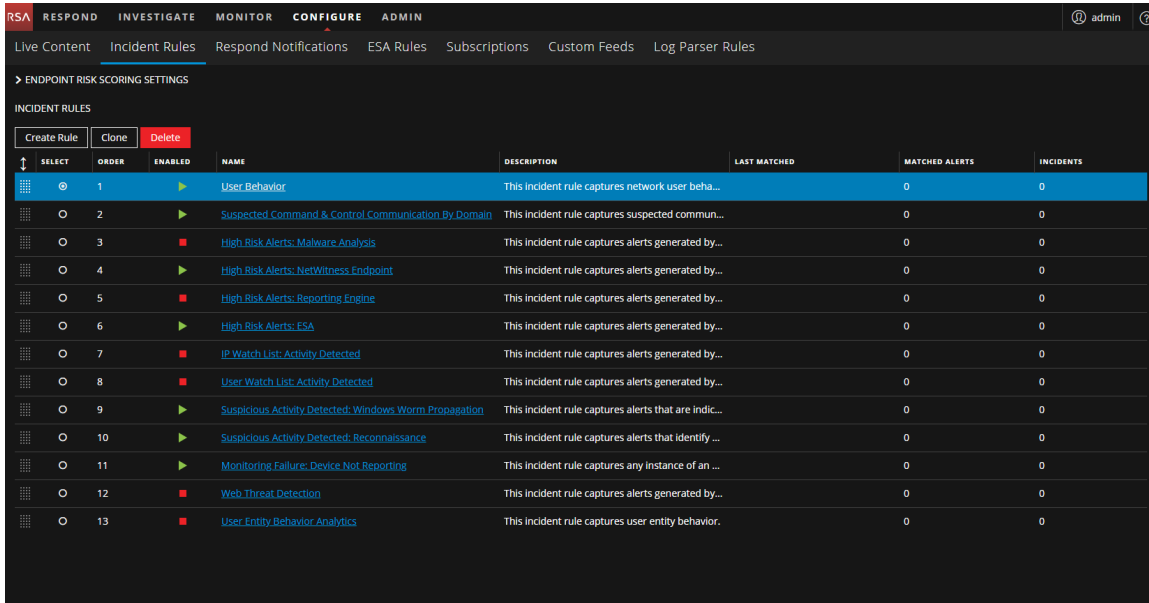
| Role                                                        | I want to ...                                                                                                                                                                                                                                                    | Show me how                                                                     |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Analyst, Content Expert, SOC Manager                        | Create or edit an incident rule.                                                                                                                                                                                                                                 | <a href="#">Step 3. Enable and Create Incident Rules for Alerts</a>             |
| Analyst, Content Expert, SOC Manager                        | Configure the threshold that creates risk scoring alerts and incidents to adjust the amount of alerts and incidents created.<br>Turn off the creation of risk scoring alerts and incidents.<br>Endpoint Risk Scoring Settings only apply to NetWitness Endpoint. | <a href="#">Configure Risk Scoring Settings for Automated Incident Creation</a> |
| Incident Responders, Analysts, Content Experts, SOC Manager | View the results of my incident rule (View Detected Threats).                                                                                                                                                                                                    | See "Responding to Incidents" in the <i>NetWitness Respond User Guide</i> .     |

### Related Topics

- [Incident Rule Details View](#)

## Quick Look

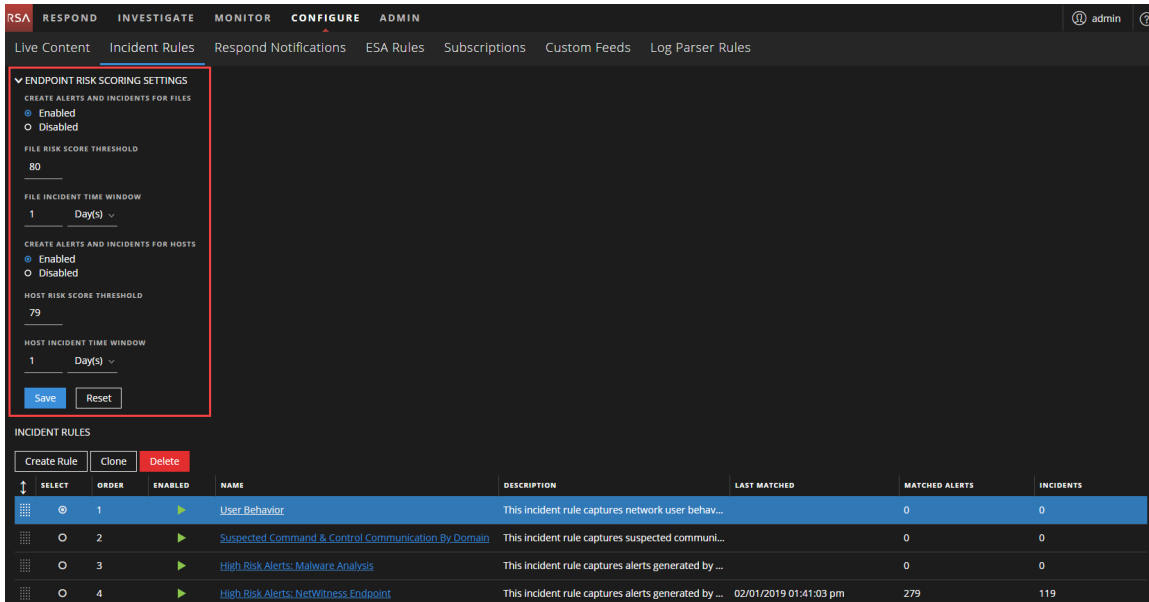
- To access the Incident Rules view, go to **CONFIGURE > Incident Rules**.



The Incident Rules view has two sections, one for each type of automated incident creation:

- Endpoint Risk Scoring Settings
- Incident Rules

- To view the Endpoint Risk Scoring Settings section, click the arrow in front of **Endpoint Risk Scoring Settings**.



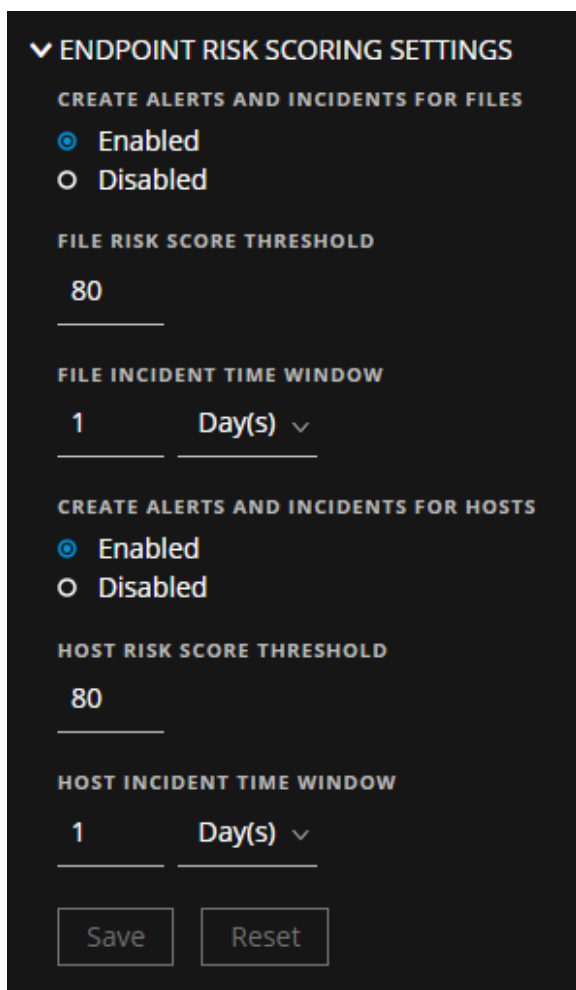


## Endpoint Risk Scoring Settings

**Note:** Endpoint Risk Scoring Settings are available in NetWitness Platform version 11.3 and later and only apply to NetWitness Endpoint. NetWitness Respond uses these settings to automatically create risk scoring incidents for suspicious files and hosts that cross the defined risk score thresholds.

The Endpoint Risk Scoring Settings enable you to configure the thresholds used to automatically create risk scoring alerts and incidents. When calculated risk scores for suspicious files and hosts exceed the specified thresholds, it triggers the creation of risk scoring alerts and incidents. RSA recommends that you keep the thresholds at the default values, but you may need to adjust these settings if you get too many or too few alerts and incidents.

For more information on configuring NetWitness Endpoint, see the *NetWitness Endpoint Configuration Guide*.



The screenshot shows a dark-themed configuration panel titled "ENDPOINT RISK SCORING SETTINGS". It is divided into two main sections: "CREATE ALERTS AND INCIDENTS FOR FILES" and "CREATE ALERTS AND INCIDENTS FOR HOSTS". Each section has a radio button to toggle between "Enabled" (selected) and "Disabled". Below each toggle are input fields for "FILE RISK SCORE THRESHOLD" and "FILE INCIDENT TIME WINDOW" (with a "Day(s)" dropdown), and "HOST RISK SCORE THRESHOLD" and "HOST INCIDENT TIME WINDOW" (with a "Day(s)" dropdown). At the bottom are "Save" and "Reset" buttons.





The following table describes the fields in the Endpoint Risk Scoring Settings.

| Field / Button                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create Alerts and Incidents for Files | <p>Select <b>Enabled</b> to automatically create risk scoring alerts and incidents for suspicious files. When calculated file risk scores go above the file risk score threshold, it triggers the creation of risk scoring alerts and incidents.</p> <p>Select <b>Disabled</b> to stop automatically creating risk scoring alerts and incidents.</p> <p>This option is enabled by default.</p>                                                                                                                                                                                                                                     |
| File Risk Score Threshold             | <p>The File Risk Score Threshold is the risk score level used to trigger alert and incident creation. The file risk score threshold range is from 0-100. NetWitness Respond calculates risk score using a combination of the number of distinct alerts and the severity of alerts associated with the file or host. A higher risk score indicates more of these types of alerts.</p> <p>For example, if the file risk score threshold is 80, any calculated file risk score over 80 creates a risk scoring alert and incident or adds a risk scoring alert to an existing incident depending on the file incident time window.</p> |
| File Incident Time Window             | <p>The File Incident Time Window is the period of time to wait before creating another incident. The file incident time window range is from 1-24 (hours or days). For example, an openme.rar file containing suspicious code with enough associated endpoint alerts to get a risk score of 81, which is over the file risk score threshold of 80, automatically creates a risk scoring alert and incident or adds a related risk scoring alert to the same incident within a 1 day time window.</p>                                                                                                                               |
| Create Alerts and Incidents for Hosts | <p>Select <b>Enabled</b> to automatically create risk scoring alerts and incidents for suspicious hosts. When calculated host risk scores go above the host risk score threshold, it triggers the creation of risk scoring alerts and incidents.</p> <p>Select <b>Disabled</b> to stop automatically creating risk scoring alerts and incidents.</p> <p>This option is enabled by default.</p>                                                                                                                                                                                                                                     |
| Host Risk Score Threshold             | <p>The Host Risk Score Threshold is the risk score level used to trigger alert and incident creation. The host risk score threshold range is from 0-100. NetWitness Respond calculates risk score using a combination of the number of distinct alerts and the severity of alerts associated with the file or host. A higher risk score indicates more of these types of alerts.</p> <p>For example, if the host risk score threshold is 80, any calculated host risk score over 80 creates a risk scoring alert and incident or adds a risk scoring alert to an existing incident depending on the host incident time window.</p> |
| Host Incident Time Window             | <p>The Host Incident Time Window is the period of time to wait before creating another incident. The host incident time window range is from 1-24 (hours or days). For example, a suspicious host with enough associated endpoint alerts to get a risk score of 81, which is over the host risk score threshold of 80, automatically creates a risk scoring alert and incident or adds a related risk scoring alert to the same incident within a 1 day time window.</p>                                                                                                                                                           |

## Incident Rules

The Incident Rules section enables you to create and manage incident rules for automating the incident creation process. NetWitness Platform provides preconfigured rules. You can add to and adjust these rules for your own environment.

The Incident Rules section consists of a list and series of buttons. The following table describes the columns in the Incident Rules list.

| Column                                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Enables you to change the priority order of the rules. Use the drag pad (  ) in front of a rule to move it up and down in the list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Select                                                                            | Enables you to select a rule in order to take an action, such as Clone or Delete.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Order                                                                             | Shows 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. If multiple rules match an alert, only the rule with the highest priority creates an incident.<br><br>NetWitness Respond evaluates incoming alerts against the incident rules in the order that you define. If alerts match the first rule listed, then that rule creates an incident. If alerts match the second rule listed and those alerts did not match the first rule, then the second rule creates an incident. If alerts match the third rule listed and those alerts did not match the first or second rule listed, then the third rule creates an incident, and so on. |
| Enabled                                                                           | Shows whether the rule is enabled or not. The  specifies that the rule is enabled. The  specifies that the rule is not enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Name                                                                              | Displays the name of the rule with a hyperlink. If you click the link, it opens the Rule Details view, where you can edit the rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Description                                                                       | Displays the description of the rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Last Matched                                                                      | Displays the time when an alert was successfully matched with the rule. 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 <a href="#">Set Counter for Matched Alerts and Incidents</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Incidents                                                                         | Displays the number of incidents created by the rule. This value is reset once a week. To change the setting, see the <a href="#">Set Counter for Matched Alerts and Incidents</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

### Incident Rules Actions

The following table shows the operations that can be performed on the Incident Rules list.

| Action                    | Description                   |
|---------------------------|-------------------------------|
| <b>Create Rule</b> button | Allows you to add a new rule. |
| <b>Delete</b> button      | Allows you to delete a rule.  |

---

| Action                | Description                     |
|-----------------------|---------------------------------|
| <b>Clone</b> button   | Allows you to duplicate a rule. |
| <b>Name</b> hyperlink | Allows you to edit a rule.      |

## Incident Rule Details View

The Incident Rule Details view enables you to create and edit incident rules for creating incidents from alerts. This topic describes the information required when creating or editing a new rule.

**Note:** The information in this topic applies to RSA NetWitness® Platform Version 11.1 and later.

### What do you want to do?

| Role                                                        | I want to ...                                                                                               | Show me how                                                                 |
|-------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Analyst, Content Expert, SOC Manager                        | Enable, create, or edit an incident rule.                                                                   | <a href="#">Step 3. Enable and Create Incident Rules for Alerts</a>         |
| Analyst, Content Expert, SOC Manager                        | Set up and use the User Behavior default rule. Set up or verify the preconfigured (default) incident rules. | <a href="#">Set Up and Verify Default Incident Rules</a>                    |
| Incident Responders, Analysts, Content Experts, SOC Manager | View the results of my incident rule (View Detected Threats).                                               | See "Responding to Incidents" in the <i>NetWitness Respond User Guide</i> . |

### Related Topics

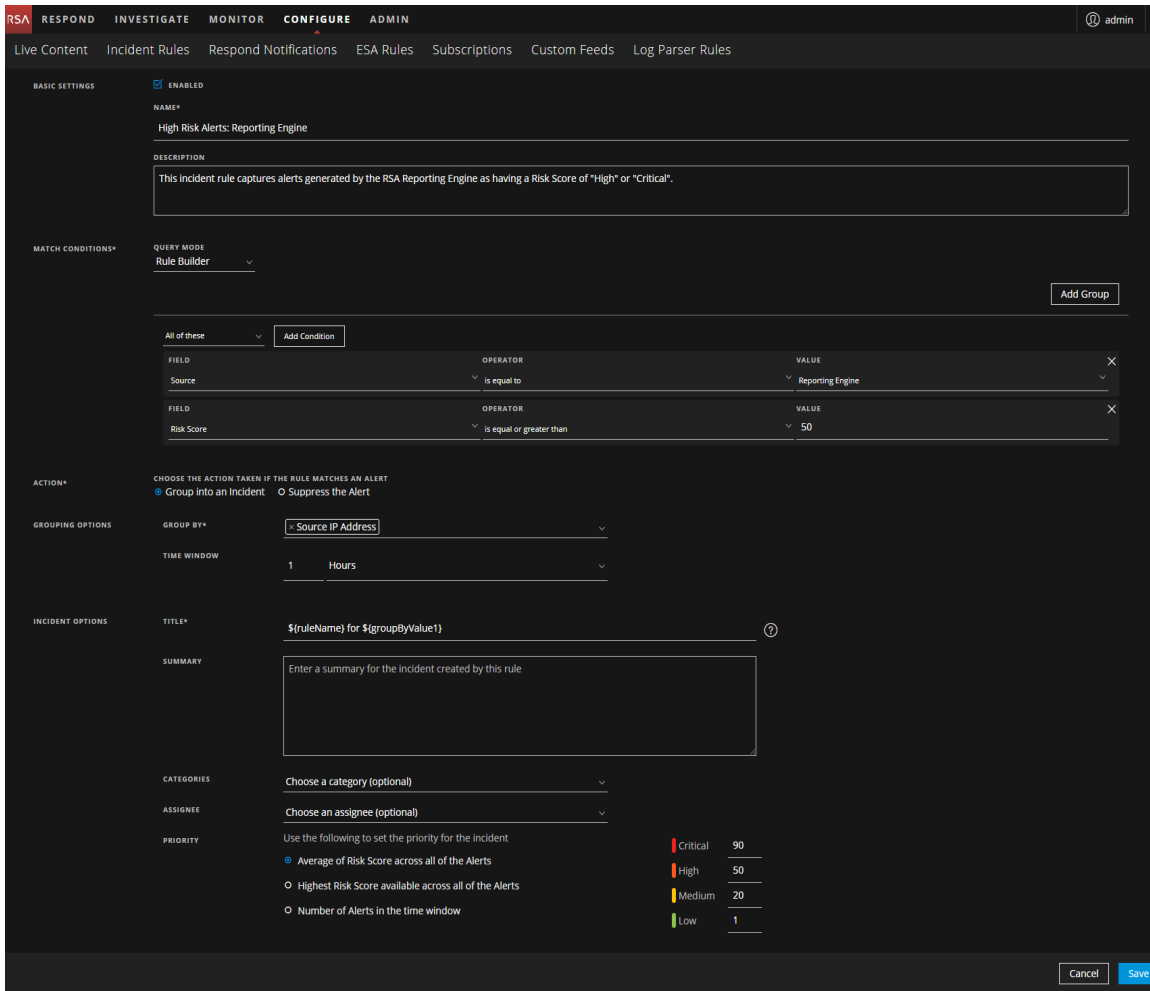
- [Incident Rules View](#)

### Quick Look

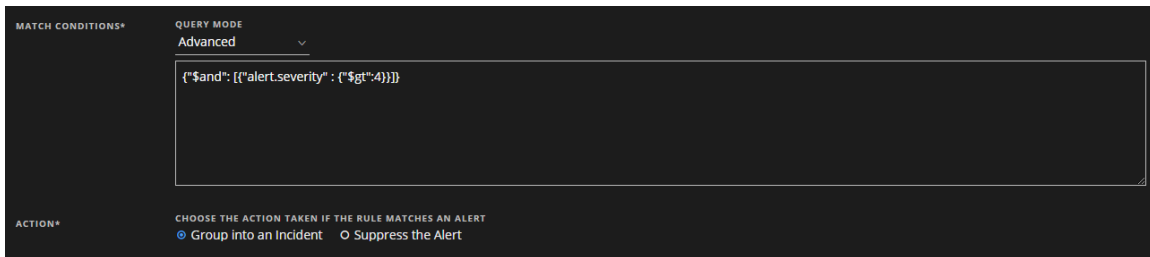
To access the Incident Rule Details view, do one of the following:

- To create a rule, go to **CONFIGURE > Incident Rules** and click **Create Rule**.
- To edit a rule, go to **CONFIGURE > Incident Rules** and click the link in the **Name** column for the rule that you want to update.

The Incident Rule Details view is displayed. The following figure shows the Incident Rule Details view in Rule Builder query mode.



In the Match Conditions section, if you select Advanced query mode, a field to enter advanced queries is available as shown in the following figure.



The following table describes the options available when creating or editing incident rules.

| Section            | Field                                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BASIC              | ENABLED                                               | Select to enable the rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SET-TINGS          | NAME*                                                 | Name of the rule. *This is a required field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                    | DESCRIP-TION                                          | A description of the rule to indicate which alerts get aggregated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| MATCH CONDI-TIONS* | QUERY MODE                                            | <p><b>Rule Builder:</b> Select the Rule Builder option if you want to build a query with various conditions that can be grouped. You can also have nested groups of conditions.</p> <p>In the Match Conditions, you can set the value to <b>All of these</b>, <b>Any of these</b>, or <b>None of these</b>. Depending on what you select, the criteria types specified in the Conditions and Group of conditions are matched to group the alerts.</p> <p>For example, if you set the match condition to <b>All of these</b>, alerts that match the criteria mentioned in the Conditions and Group Conditions are grouped into one incident.</p> <ul style="list-style-type: none"> <li>• Add a Condition to be matched by clicking the <b>Add Condition</b> button.</li> <li>• Add a Group of Conditions by clicking the <b>Add Group</b> button and add conditions by clicking the <b>Add Condition</b> button.</li> </ul> <p>You can include multiple Conditions and Groups of Conditions that can be matched as per criteria set and group the incoming alerts into incidents.</p> <p><b>Advanced:</b> Select the Advanced query option if you want to use the advanced query builder. You can add a specific condition that needs to be matched as per the matching option selected.</p> <p>For example, you can type the criteria builder format <code>{"\$and": [{"alert.severity" : {"\$gt":4}}]}</code> to group alerts that have severity greater than 4.</p> <p>For advanced syntax, refer to <a href="http://docs.mongodb.org/manual/reference/operator/query/">http://docs.mongodb.org/manual/reference/operator/query/</a> or <a href="http://docs.mongodb.org/manual/reference/method/db.collection.find/">http://docs.mongodb.org/manual/reference/method/db.collection.find/</a></p> |
| AC-TION*           | CHOOSE THE ACTION TAKEN IF THE RULE MATCHES THE ALERT | <p><b>Group into an Incident:</b> If enabled, the alerts that match the criteria set are grouped into an alert.</p> <p><b>Suppress the Alert:</b> If enabled, the alerts that match the criteria are suppressed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Section                       | Field          | Description                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GROUP-<br>ING<br>OP-<br>TIONS | GROUP<br>BY*   | The criteria to group the alerts in accordance with the specified alert fields. You can use a maximum of two fields to group the alerts. You cannot group alerts with fields that do not have values. When alerts are grouped on an alert field, all matching alerts containing the same meta key value for that field are grouped together in the same incident. (See the following <b>Group By Meta Key Mappings</b> table.) |
|                               | TIME<br>WINDOW | The time range for grouping alerts.<br>For example, if the time window is set to 1 hour, all alerts that match the criteria set in the Group By field and that arrive within an hour of each other are grouped into an incident.                                                                                                                                                                                               |



| Section          | Field      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| INCIDENT OPTIONS | TITLE*     | <p>Title of the incident. You can optionally include placeholders in your title. Placeholders enable you to have different titles based on the attributes you grouped. If you do not use placeholders, all incidents created by the rule will have the same title.</p> <p>For example, if you grouped them according to the source, you can name the resulting Incident as Alerts for <b>\${groupByValue1}</b>, and the incident for all alerts from NetWitness Endpoint would be named <b>Alerts for NetWitness Endpoint</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                        |
|                  | SUMMARY    | (Optional) Summary of the incident created by this rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                  | CATEGORIES | (Optional) Category of the incident created. An incident can be classified using more than one category.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                  | ASSIGNEE   | (Optional) Name of the user assigned to the incident.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                  | PRIORITY   | <p><b>Average of Risk Score across all of the Alerts:</b> Takes the average of the risk scores across all the alerts to set the priority of the incident created.</p> <p><b>Highest Risk Score available across all of the Alerts:</b> Takes the highest score available across all the alerts to set the priority of the incident created.</p> <p><b>Number of Alerts in the time window:</b> Takes the count of the number of alerts in the time window selected to set the priority of the incident created.</p> <p><b>Critical, High, Medium, and Low:</b> Specify the incident priority threshold of the matched incidents. The defaults are:</p> <ul style="list-style-type: none"> <li>• Critical: 90</li> <li>• High: 50</li> <li>• Medium: 20</li> <li>• Low: 1</li> </ul> <p>For example, with the Critical priority set to 90, incidents with a risk score of 90 or higher are assigned a Critical priority for this rule.</p> |

## Group By Meta Key Mappings

When alerts are grouped on an alert field, all matching alerts containing the same meta key value for that field are grouped together in the same incident. For example, if you select the Group By field value **Destination Host**, it uses the mapped meta key `alert.groupby_host_dst`. All alerts with the same meta key value for `alert.groupby_host_dst` are grouped together in the same incident.

The following table shows the mapped meta keys for the Group By field selections.

| Group By Field Value     | Mapped Meta Key                   |
|--------------------------|-----------------------------------|
| Alert Name               | alert.name                        |
| Alert Rule Id            | alert.signature_id                |
| Alert Type               | alert.groupby_type                |
| Date Created             | alert.timestamp                   |
| Destination Country      | alert.groupby_destination_country |
| Destination Domain       | alert.groupby_domain_dst          |
| Destination Host         | alert.groupby_host_dst            |
| Destination IP Address   | alert.groupby_destination_ip      |
| Destination Port         | alert.groupby_destination_port    |
| Destination User Account | alert.groupby_user_dst            |
| Detector IP Address      | alert.groupby_detector_ip         |
| Domain                   | alert.groupby_domain              |
| Domain for Suspected C&C | alert.groupby_c2domain            |
| File Analysis            | alert.groupby_analysis_file       |
| Filename                 | alert.groupby_filename            |
| File MD5 Hash            | alert.groupby_data_hash           |
| Risk Score               | alert.risk_score                  |
| Service Analysis         | alert.groupby_analysis_service    |
| Session Analysis         | alert.groupby_analysis_session    |
| Severity                 | alert.severity                    |
| Source                   | alert.source                      |
| Source Country           | alert.groupby_source_country      |
| Source Domain            | alert.groupby_domain_src          |
| Source Host              | alert.groupby_host_src            |
| Source IP Address        | alert.groupby_source_ip           |
| Source User Account      | alert.groupby_user_src            |
| Source Username          | alert.groupby_source_username     |
| User Account             | alert.groupby_username            |

## Respond Notification Settings View

The Respond Notification Settings view enables you to send email notifications when incidents are created or updated to SOC Managers and the Analysts assigned to the incidents.

**Note:** The information in this topic applies to RSA NetWitness® Platform 11.1 and later.

### What do you want to do?

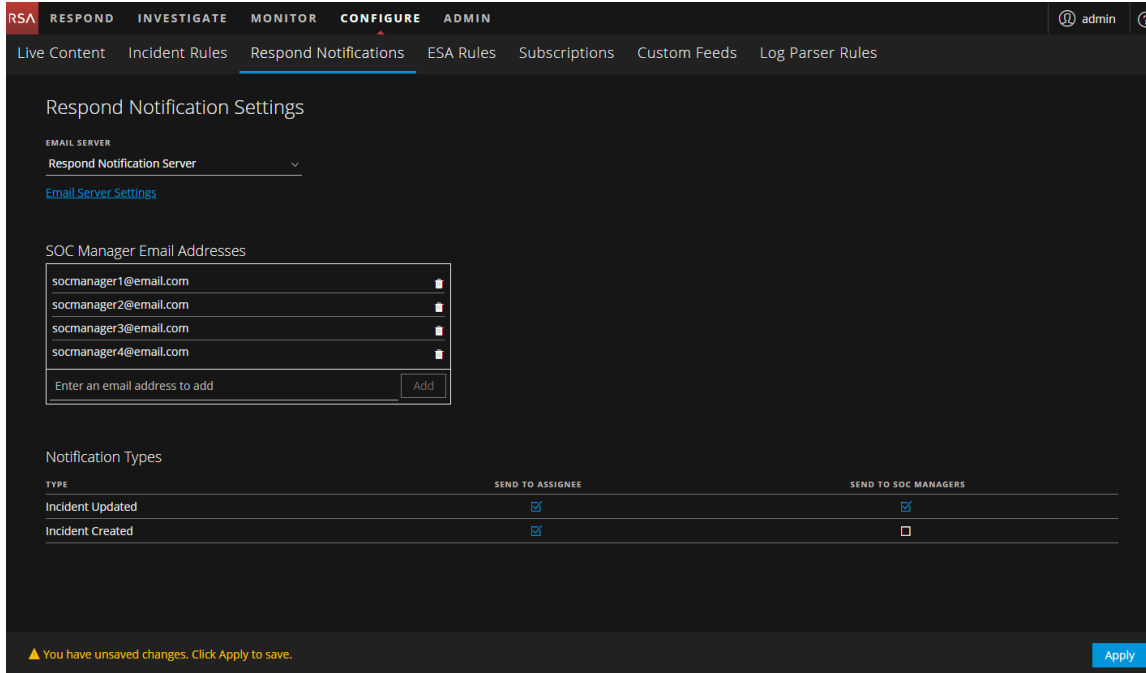
| Role                                                        | I want to ...                                                             | Show me how                                                                                                                                                                                                                                     |
|-------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrator                                               | Configure an email server.                                                | Refer to "Configure the Email Settings as Notification Server" in the <i>System Configuration Guide</i> . (To access these settings, click the <b>Email Server Settings</b> link or go to ADMIN > System > Global Notifications > Servers tab.) |
| Incident Responders, Analysts, Content Experts, SOC Manager | Configure email notifications for when an incident is created or updated. | <a href="#">Configure Respond Email Notification Settings</a>                                                                                                                                                                                   |

### Related Topics

- [Incident Rules View](#)

### Quick Look

To access the Respond notification settings, go to **CONFIGURE > Respond Notifications**. The Respond Notification Settings view is displayed.



The following table lists the Respond notification settings.

| Setting                               | Description                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Email Server                          | Specifies the Email server that will send the email notifications.                                                                                                                                                                                                                                                                                                                                           |
| Email Server Settings                 | Allows you to configure an Email server if the one you want to use for notifications is not listed.<br>Clicking the <b>Email Server Settings</b> link goes to ADMIN > SYSTEM > Global Notifications. For instructions, refer to "Configure the Email Settings as Notification Server" in the <i>System Configuration Guide</i> .                                                                             |
| SOC Manager Email Addresses           | Lists the SOC Manager email addresses that receive email notifications when you select <b>Send to SOC Manager</b> in the Notification Types section. You can add and remove email addresses as needed.                                                                                                                                                                                                       |
| Notification Types - Incident Created | Specifies who should receive an email notification when an incident is created. <ul style="list-style-type: none"> <li><b>Send to Assignee:</b> When an incident is created, an email is sent to the Analyst assigned to the incident.</li> <li><b>Send to SOC Manager:</b> When an incident is created, an email is sent to all of the addresses listed in the SOC Manager Email Addresses list.</li> </ul> |

| Setting                               | Description                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Notification Types - Incident Updated | <p>Specifies who should receive an email notification when an incident is created.</p> <ul style="list-style-type: none"> <li>• <b>Send to Assignee:</b> When an incident is updated, an email is sent to the Analyst assigned to the incident.</li> <li>• <b>Send to SOC Manager:</b> When an incident is updated, an email is sent to all of the addresses listed in the SOC Manager Email Addresses list.</li> </ul> |
| Apply                                 | <p>Applies changes made to Respond Notification Settings. Changes to these settings take effect immediately.</p>                                                                                                                                                                                                                                                                                                        |

**Note:** If user email address information is updated in the ADMIN > Security > Users tab, it can take up to two minutes for the new email changes to take effect. Any incident creation or incident update email notifications sent during this time go to the old email address.

## Aggregation Rules Tab

The Aggregation Rules tab enables you to create and manage aggregation rules for automating the incident creation process. NetWitness Platform provides 11 preconfigured rules. You can add to and adjust these rules for your own environment.

**Note:** This topic applies to NetWitness Platform version 11.0 and earlier.

### What do you want to do?

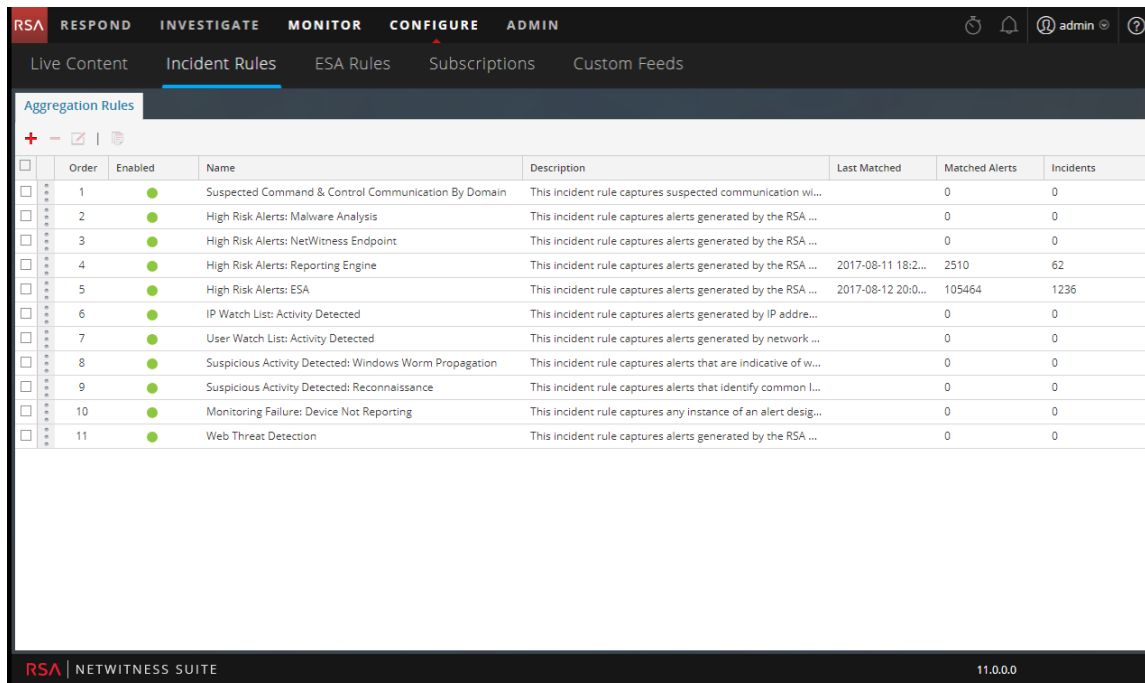
| Role                                                        | I want to ...                                                    | Show me how                                                                 |
|-------------------------------------------------------------|------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Analyst, Content Expert, SOC Manager                        | Create an aggregation rule.                                      | <a href="#">Step 3. Enable and Create Incident Rules for Alerts</a>         |
| Incident Responders, Analysts, Content Experts, SOC Manager | View the results of my aggregation rule (View Detected Threats). | See "Responding to Incidents" in the <i>NetWitness Respond User Guide</i> . |

### Related Topics

- [New Rule Tab](#)

### Quick Look


To access the Aggregation Rules tab, go to **CONFIGURE > Incident Rules > Aggregation Rules** tab.



The Aggregation Rules tab consists of a list and toolbar.





## Aggregation Rules List

The following table describes the columns in the Aggregation Rules list.

| Column         | Description                                                                                                                                                                                                                                |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Select         | Enables you to select a rule in order to take an action, such as Clone or Delete.                                                                                                                                                          |
| Order          | Shows 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. If two rules match an alert, only the rule with the highest priority is evaluated. |
| Name           | Displays the name of the rule.                                                                                                                                                                                                             |
| Enabled        | Shows whether the rule is enabled or not. The  specifies the rule is enabled.                                                                             |
| Description    | Displays the description of the rule.                                                                                                                                                                                                      |
| Last Matched   | Displays the time when an alert was successfully matched with the rule. 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 <a href="#">Set Counter for Matched Alerts and Incidents</a> .                                                                          |
| Incidents      | Displays the number of incidents created by the rule. This value is reset once a week. To change the setting, see the <a href="#">Set Counter for Matched Alerts and Incidents</a> .                                                       |

## Aggregation Rules Toolbar

The following table shows the operations that can be performed in the Aggregation Rules tab.

| Option                                                                              | 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

The New Rules tab enables you to create custom aggregation rules for automating the incident creation process. This topic describes the information required when creating a new rule.

**Note:** This topic applies to NetWitness Platform version 11.0 and earlier.

### What do you want to do?

| Role                                                        | I want to ...                                                    | Show me how                                                                 |
|-------------------------------------------------------------|------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Analyst, Content Expert, SOC Manager                        | Create an aggregation rule.                                      | <a href="#">Step 3. Enable and Create Incident Rules for Alerts</a>         |
| Incident Responders, Analysts, Content Experts, SOC Manager | View the results of my aggregation rule (View Detected Threats). | See "Responding to Incidents" in the <i>NetWitness Respond User Guide</i> . |

### Related Topics

- [Aggregation Rules Tab](#)

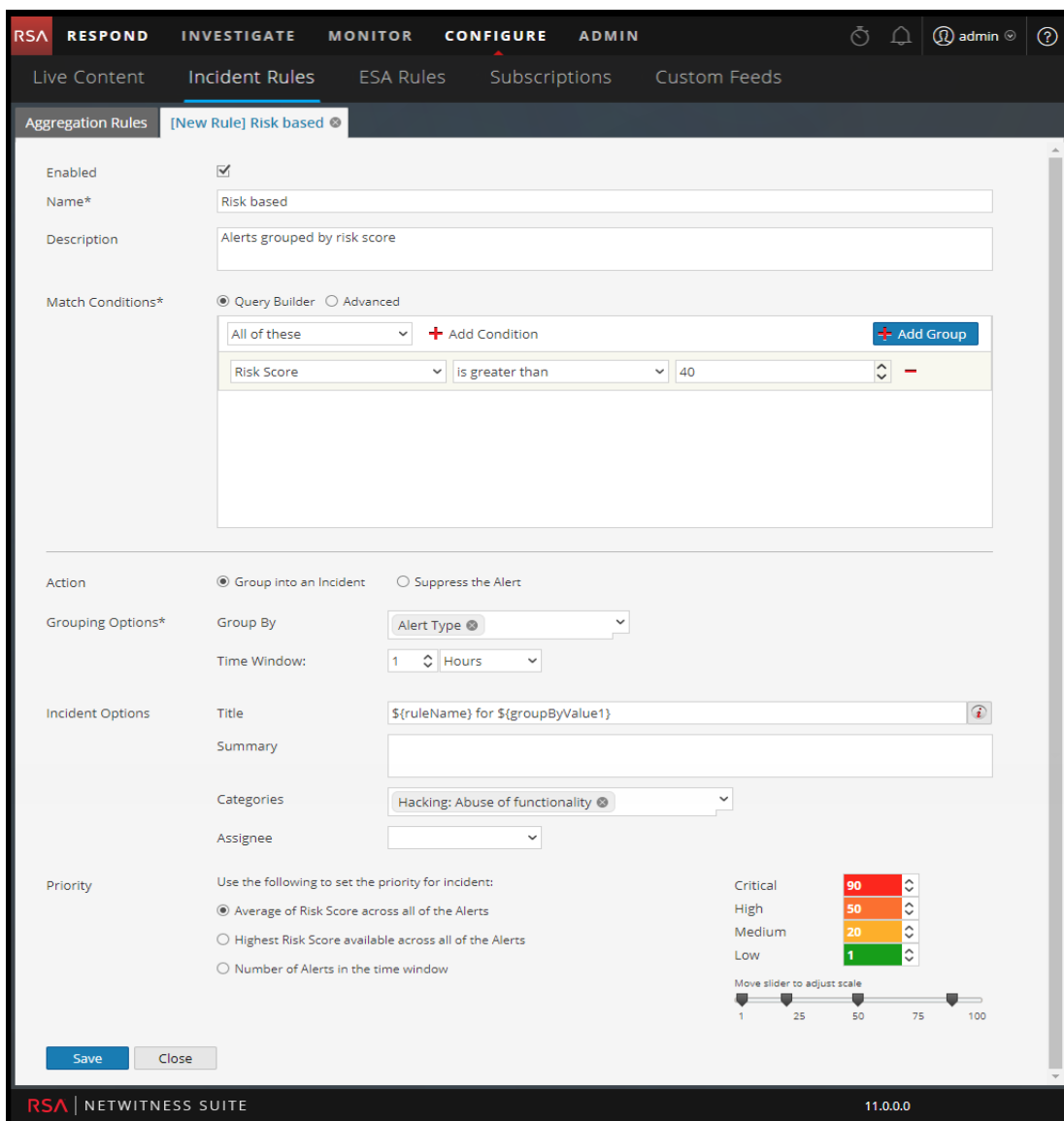
### Quick Look

To access the New Rule tab view:

1. Go to **CONFIGURE > Incident Rules > Aggregation Rules** tab.
2. Click **+**.






The **New Rule** tab is displayed.



The following table describes the options available when creating customized aggregation rules.

| Field       | 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. |

| Field             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Match Conditions* | <p><b>Query Builder</b> - Select if you want to build a query with various conditions that can be grouped. You can also have nested groups of conditions.</p> <p>Match Conditions - You can set the value to <b>All of these</b>, <b>Any of these</b>, or <b>None of these</b>. Depending on what you select, the criteria types specified in the Conditions and Group of conditions are matched to group the alerts.</p> <p><b>For example</b>, if you set the match condition to <b>All of these</b>, alerts that match the criteria mentioned in the Conditions and Group Conditions are grouped into one incident.</p> <ul style="list-style-type: none"> <li>• Add a Condition to be matched by clicking  <b>Add Condition</b>.</li> <li>• Add a Group of Conditions by clicking  <b>Add Group</b> and adding conditions by clicking  <b>Add Condition</b>.</li> </ul> <p>You can include multiple Conditions and Groups of Conditions that can be matched as per criteria set and group the incoming alerts into incidents.</p> <p><b>Advanced</b> - 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.</p> <p><b>For example:</b> you can type the criteria builder format <code>{"\$and": [{"alert.severity" : {"\$gt":4}}]}</code> to group alerts that have severity greater than 4.</p> <p>For advanced syntax, refer to <a href="http://docs.mongodb.org/manual/reference/operator/query/">http://docs.mongodb.org/manual/reference/operator/query/</a> or <a href="http://docs.mongodb.org/manual/reference/method/db.collection.find/">http://docs.mongodb.org/manual/reference/method/db.collection.find/</a></p> |
| Action            | <p><b>Group into an Incident</b> - If enabled, the alerts that match the criteria set are grouped into an alert.</p> <p><b>Suppress the Alert</b> - If enabled, the alerts that match the criteria are suppressed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Grouping Options* | <p><b>Group By:</b> The criteria to group the alerts as per the specified category. You can use a maximum of two attributes to group the alerts. You can group the alerts with one or two attributes. You can no longer group alerts with attributes that do not have values (empty attributes).</p> <p>Grouping on an attribute means that all matching Alerts containing the same value for that attribute are grouped together in the same incident.</p> <p><b>Time Window:</b> The time range specified to group alerts.</p> <p>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.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Incident Options | <p><b>Title</b> - (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.</p> <p>For example, if you grouped them according to the source, you can name the resulting Incident as Alerts for <b>`\${groupByValue1}`</b>, and the incident for all alerts from NetWitness Endpoint would be named <b>Alerts for NetWitness Endpoint</b>.</p> <p><b>Summary</b> - (Optional) Summary of the incident.</p> <p><b>Category</b> - (Optional) Category of the incident created. An incident can be classified using more than one category.</p> <p><b>Assignee</b> - (Optional) Name of the assignee to whom the incident is assigned to.</p>                                                                                                                                                                                                                                                                                   |
| Priority         | <p><b>Average of Risk Score across all of the Alerts</b> - Takes the average of the risk scores across all the alerts to set the priority of the incident created.</p> <p><b>Highest Risk Score available across all of the Alerts</b> - Takes the highest score available across all the alerts to set the priority of the incident created.</p> <p><b>Number of Alerts in the time window</b> - Takes the count of the number of alerts in the time window selected to set the priority of the incident created.</p> <p><b>Critical, High, Medium, and Low</b> - Specify the incident priority threshold of the matched incidents. The defaults are:</p> <ul style="list-style-type: none"> <li>• Critical: 90</li> <li>• High: 50</li> <li>• Medium: 20</li> <li>• Low: 1</li> </ul> <p>For example, with the Critical priority set to 90, incidents with a risk score of 90 or higher will be assigned a Critical priority for this rule.</p> <p>You can change these defaults by manually changing the priorities or by moving the slider under <b>Move slider to adjust scale</b>.</p> |