RSA NETWITNESS® PLATFORM

NetWitness Respond Configuration Guide

for Version 11.2

Contact Information

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

Trademarks

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

License Agreement

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

August 2018

Contents

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

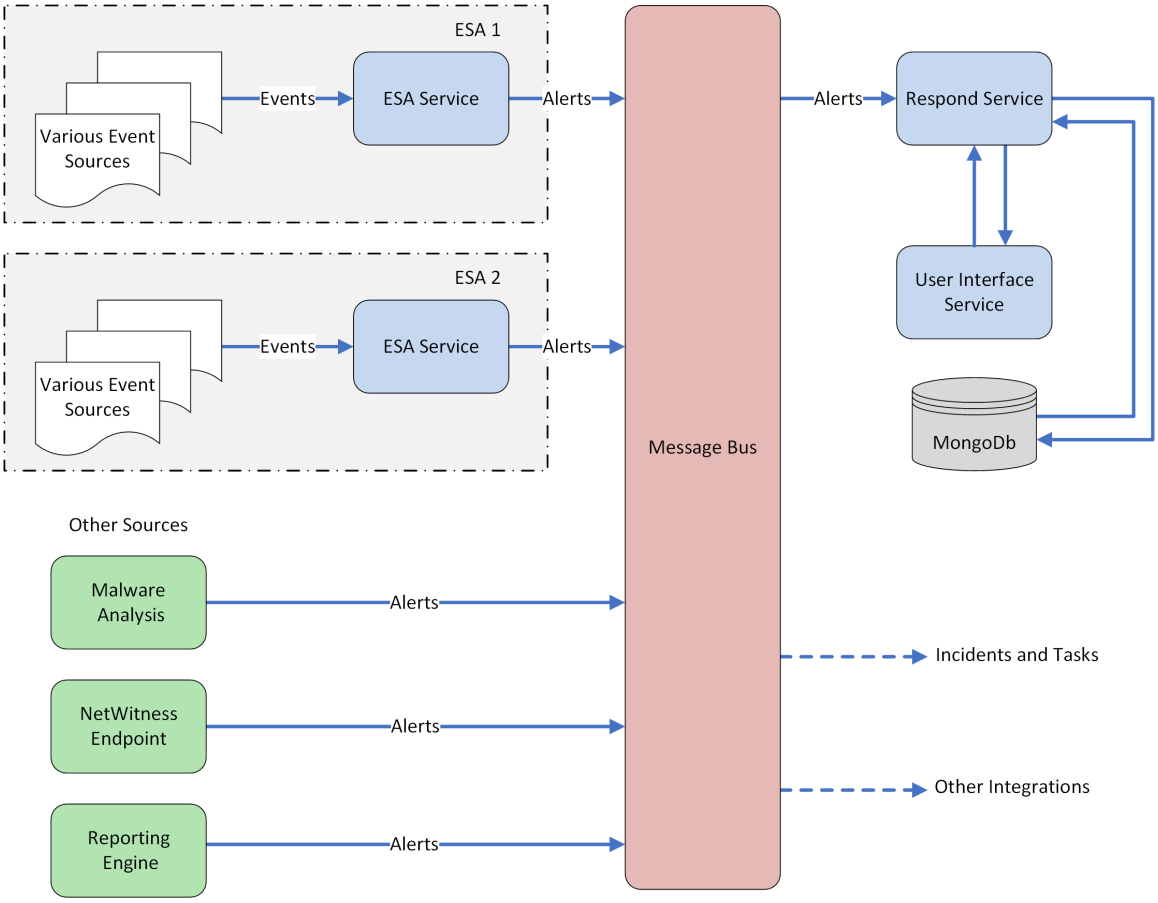
NetWitness Respond Configuration Overview

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

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:

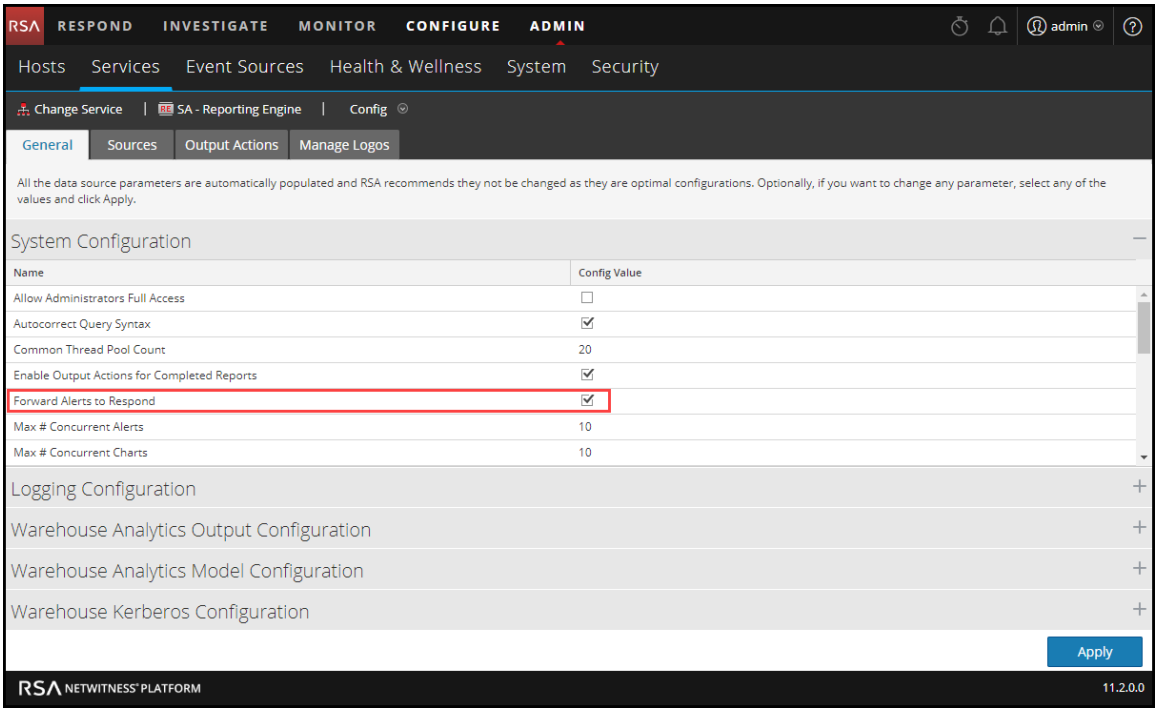
- The Respond Server service is installed and running on NetWitness Platform.
- NetWitness Endpoint is installed and running. This is necessary only if you want to configure NetWitness Endpoint as an alert source in the Respond view.

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**.



   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

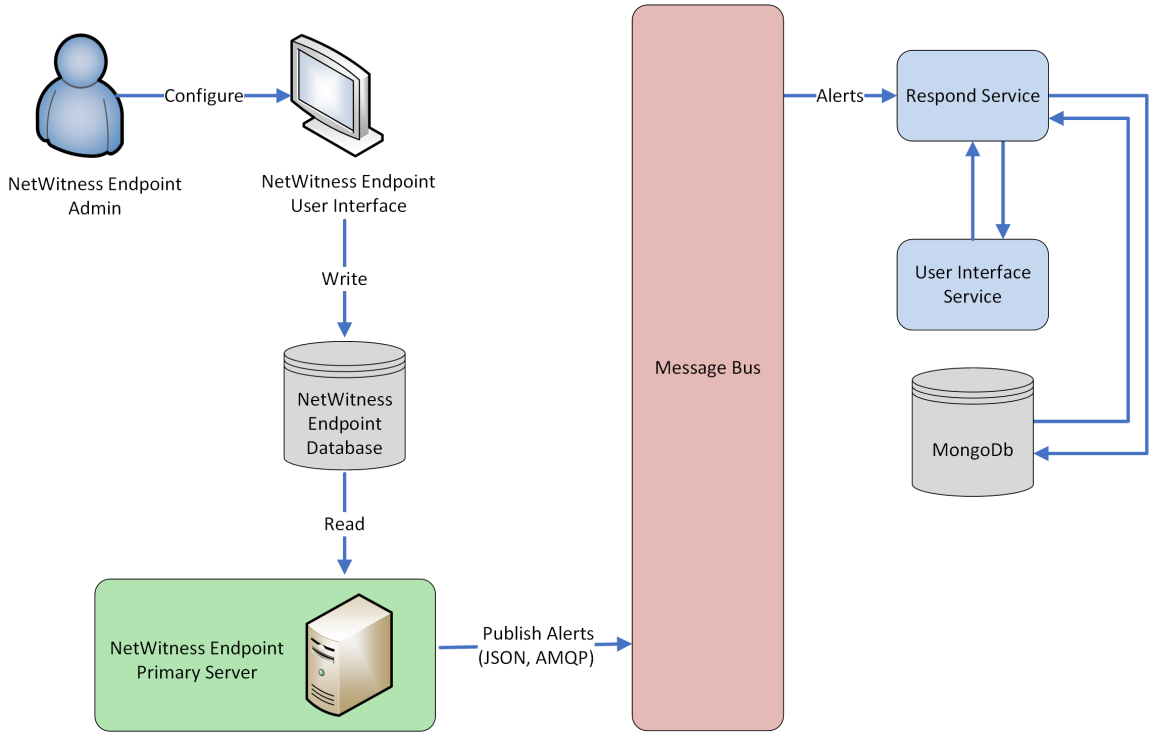
Viewing NetWitness Respond alerts is a function of auditing in Malware Analysis. The procedure of enabling NetWitness Respond alerts is described in the "(Optional) Configure Auditing on Malware Analysis Host" topic in the *Malware Analysis Configuration Guide*.

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, or later for NetWitness Respond integration. For more detailed information, see "RSA NetWitness Platform Integration" in the *NetWitness Endpoint User Guide*.

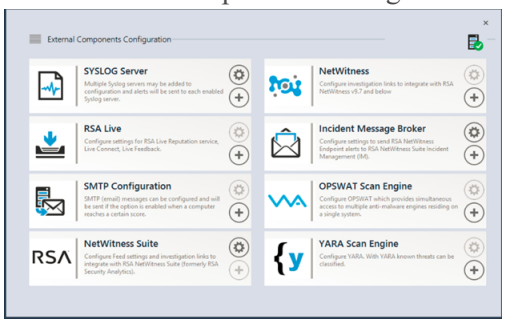
The diagram below represents the flow of NetWitness Endpoint alerts to the NetWitness Platform Respond Server service and its display in the **RESPOND > Alerts** view.



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 (Available in 11.1 and later)		Yes	Yes*	Yes*		
respond-server.notification.read (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

Permissions	Analysts	SOC Mgrs	DPOs	Respond Admin	Operators	MAs
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 Investigate Server permissions are required to view Event Analysis in the Respond view:

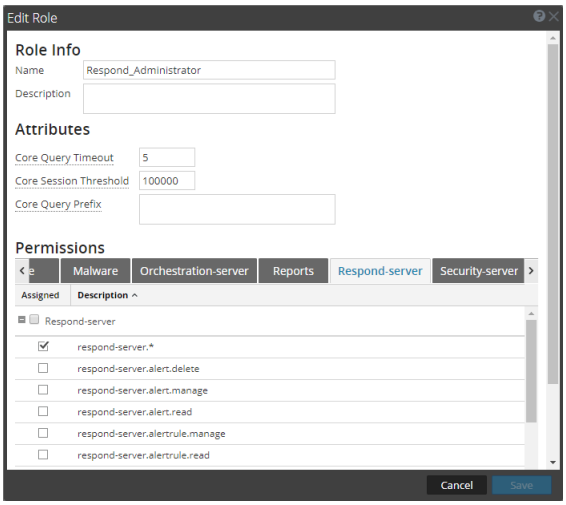
Investigate-server tab:

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

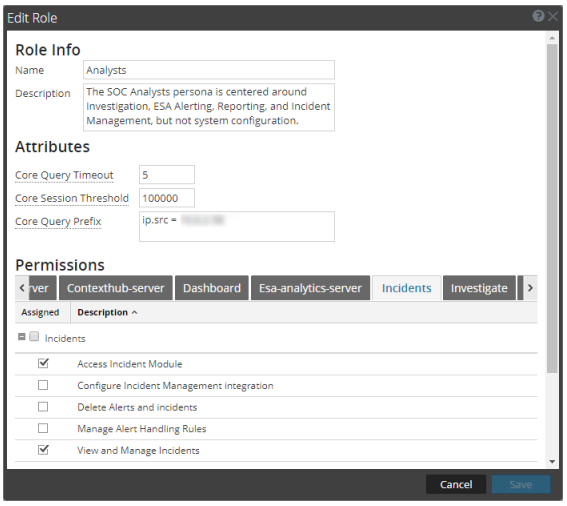
Note: Migrated incidents from NetWitness Platform versions before 11.2 will not show the Event Analysis panel in the Respond Incident Details view Indicators panel. Likewise, if you use alerts that were migrated from versions before 11.2 to create incidents in 11.2, you will also not be able to view 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 12 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 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.

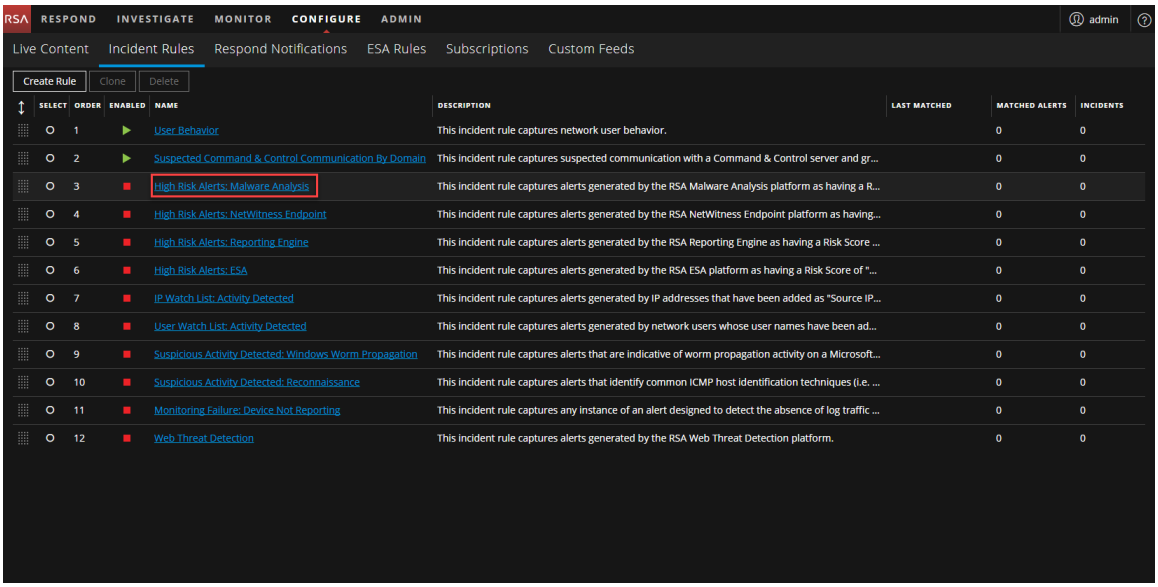
Some predefined (default) incident rules changed slightly in 11.1 and later. To verify your existing default incident rules with the 11.2 default incident rules, see Set Up and Verify Default Incident Rules.

Enable an Incident Rule

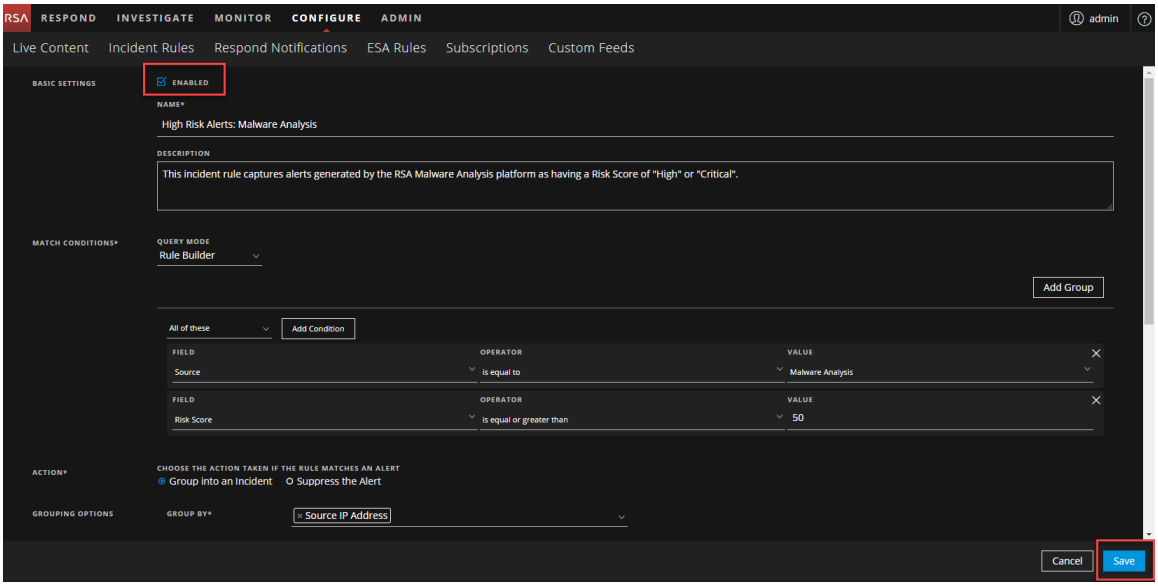
To create incidents automatically, you need to enable at least one incident rule. Predefined (default) incident rules or rules that you create must be enabled before they start creating incidents.

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

   The Incident Rules List view is displayed. The example below shows the 12 default incident rules.

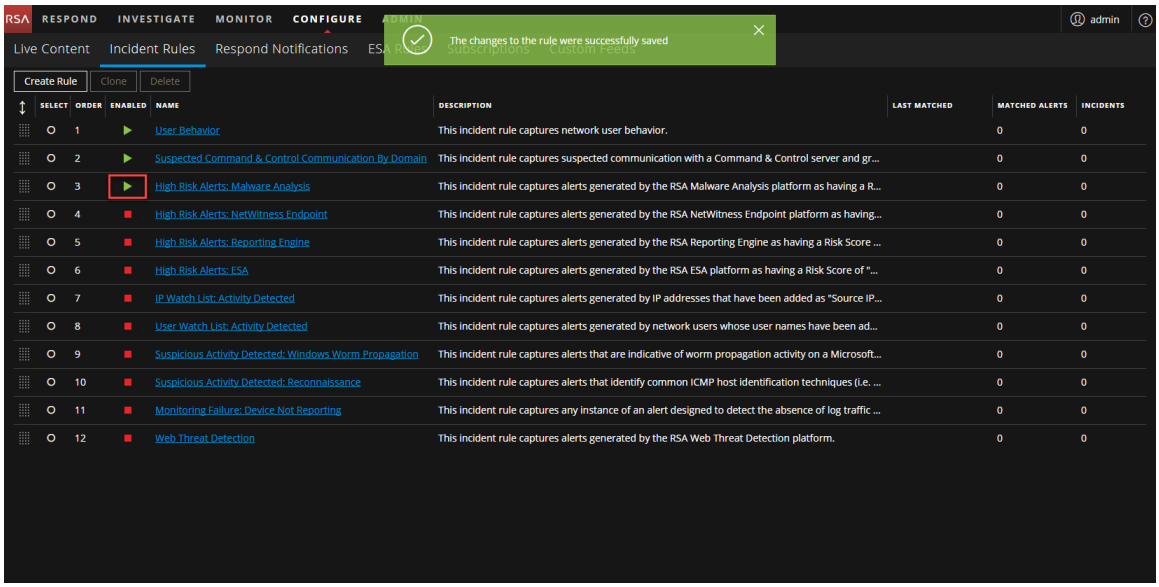


2. Click the link in the **Name** column for the rule that you want to enable.
   The Incident Rule Details view is displayed for the selected rule.



3. 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.
4. In the Basic Settings section, select **Enabled**.

5. Click **Save** to enable the rule.
   Notice that the Enabled column changes from a red square ■ (Disabled) to green triangle ▶ (Enabled).

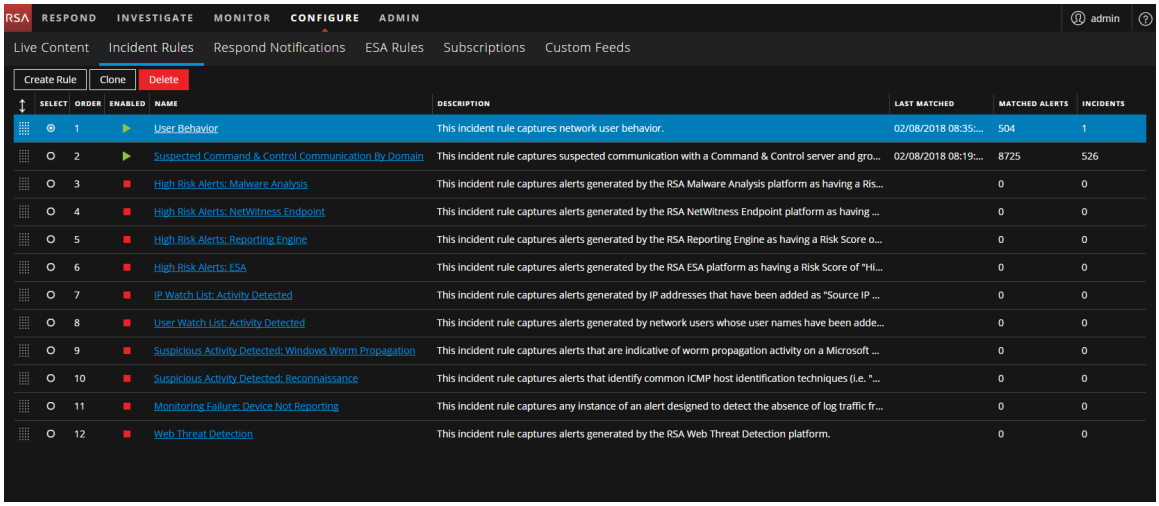


6. Verify the order of your incident rules.

Create an Incident Rule

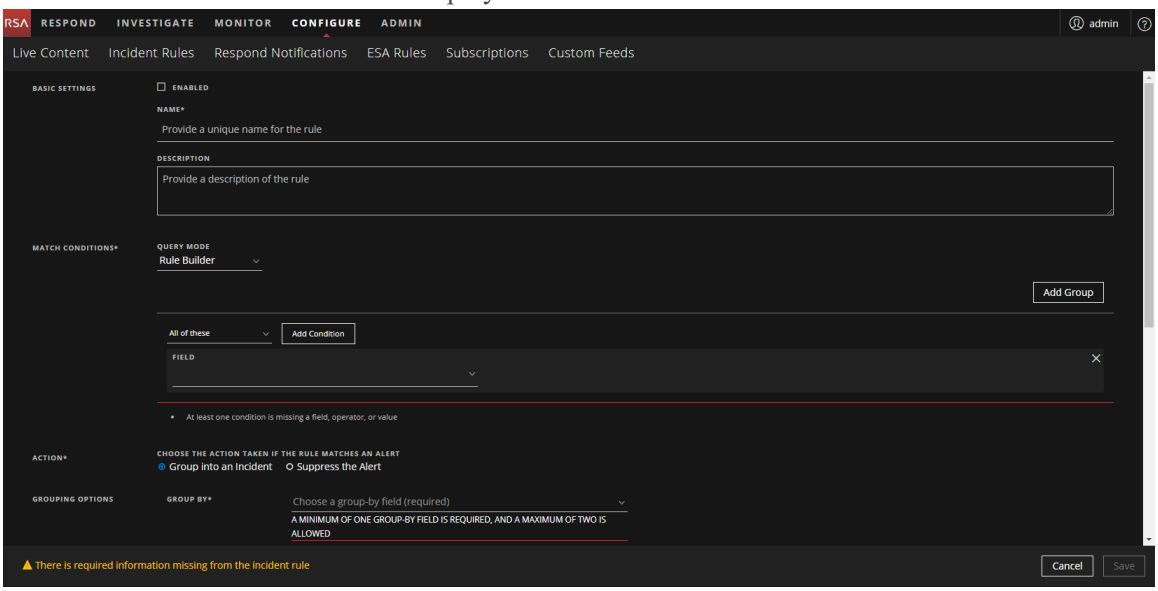
1. Go to **CONFIGURE > Incident Rules**.

   The Incident Rules List view is displayed.



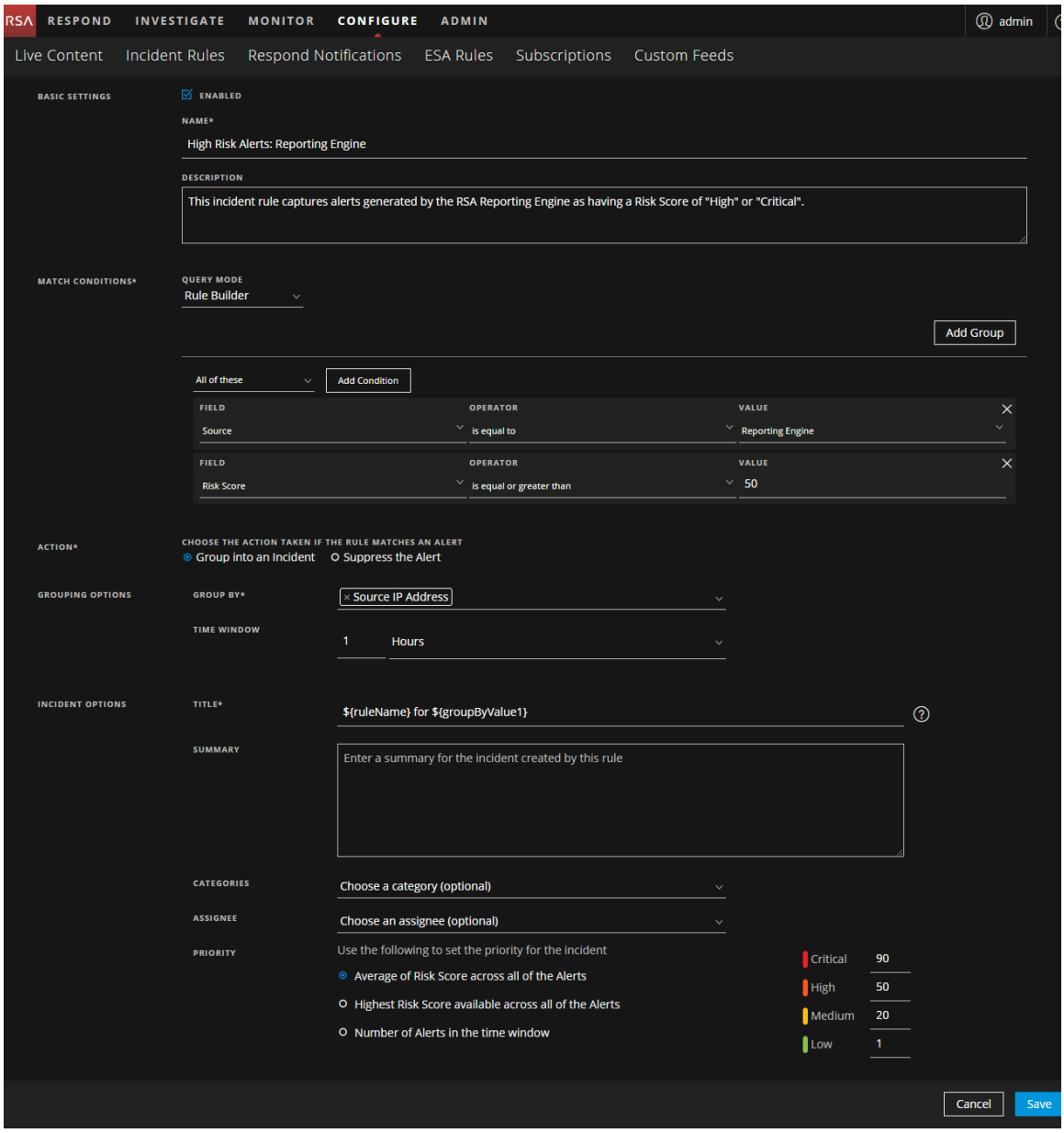
2. To add a new rule, click **Create Rule**.

The Incident Rule Details view is displayed.



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

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 two rules match an alert, only the rule with the highest priority is evaluated.

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 List 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 various 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 view, see Incident Rules List 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 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
- Set Counter for Matched Alerts and Incidents
- Configure a Database for the Respond Server Service

Set Up and Verify Default Incident Rules

The User Behavior incident rule, which captures network user behavior, was introduced in NetWitness Platform 11.1. 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: NetWitness Endpoint*
- High Risk Alerts: ESA

*To aggregate NetWitness Endpoint alerts based on the Detector IP Address, create another NetWitness Endpoint Rule using the Detector IP Address as the Group By value. See Create a NetWitness Endpoint Incident Rule using Detector IP for step-by-step instructions.

To verify your existing default incident rules with the 11.2 default incident rules, look at the default incident rule tables following these procedures.

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**.

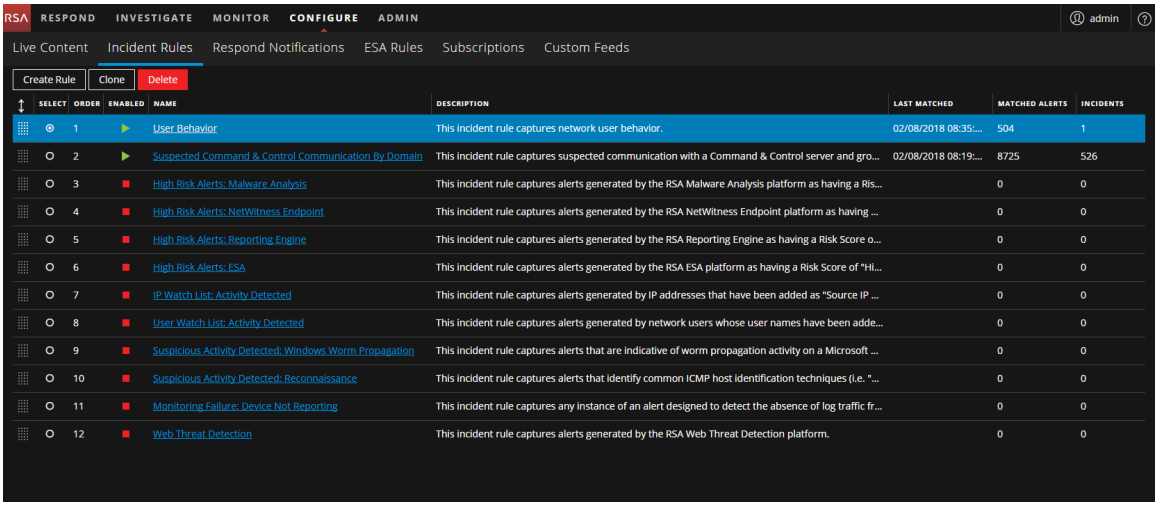
5. To add a new Deployment, in the drop-down list near **DEPLOYMENTS**, click **Add**.
   a. In the ESA Services section, add and then select your ESA service.
   b. In the ESA Rules section, click + and in the Deploy ESA Rules dialog, select the ESA Rules that you selected from the **User Behavior** 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:

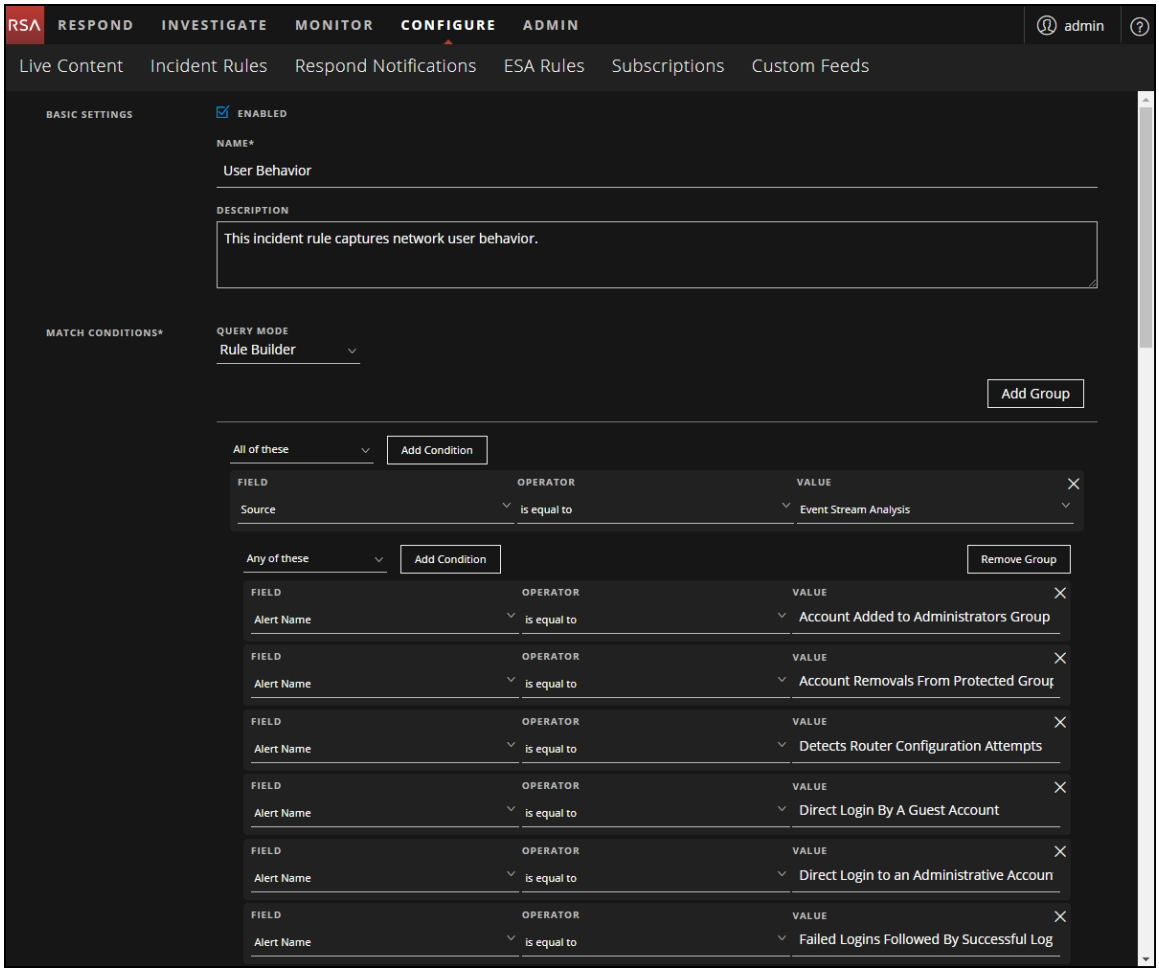
1. Go to **CONFIGURE > Incident Rules.**
   The Incident Rules List view is displayed.



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.



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.

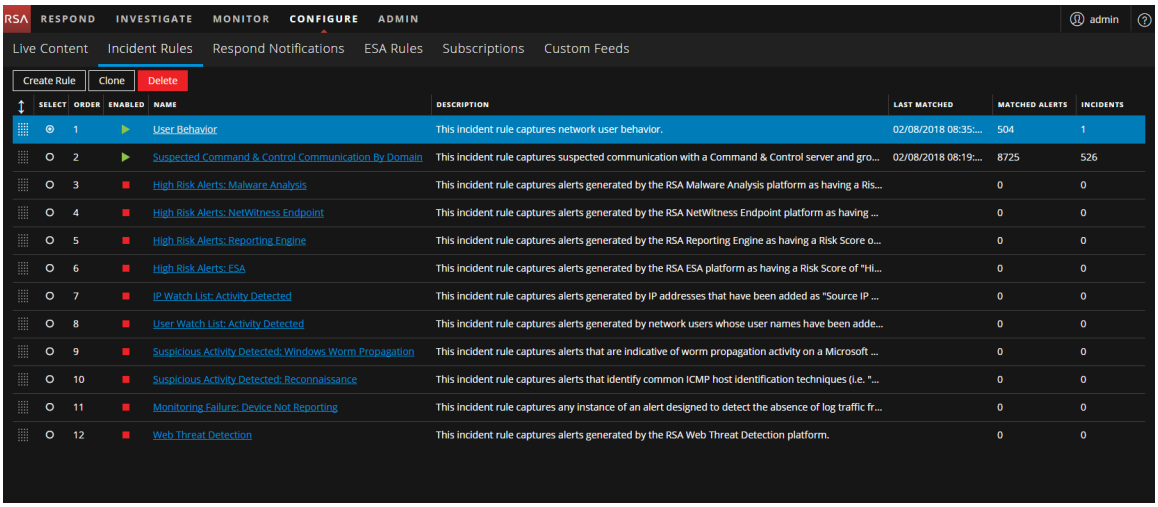
Field	Condition Field	Condition Operator	Value
Name			User Behavior
Description			This incident rule captures network user behavior.
1st Group:			All of these
Condition:	Source	is equal to	Event Stream Analysis
2nd Group:			Any of these
Conditions:	Alert Name	is equal to	Account Added to Administrators 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

Field	Condition Field	Condition Operator	Value
	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
	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

Field	Condition Field	Condition Operator	Value
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 List view is displayed.



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 Command & Control Communication By Domain default incident rule.

Field	Condition Field	Condition Operator	Value
Name			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			NetWitness Platform detected communications with ${groupByValue1} that may be command and control malware. 1. Evaluate if the domain is legitimate (online radio, news feed, partner, automated testing, etc.). 2. Review the domain registration for suspect information (Registrant country, registrar, no registration data found, etc). 3. If the domain is suspect, go to the Investigation module to locate other activity to or from it.

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

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}

*To aggregate NetWitness Endpoint alerts based on the Detector IP Address, create another NetWitness Endpoint Rule using the Detector IP Address as the Group By value. See Create a NetWitness Endpoint Incident Rule using Detector IP 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
	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

Field	Condition Field	Condition Operator	Value
	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

Field	Condition Field	Condition Operator	Value
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 Logs
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
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

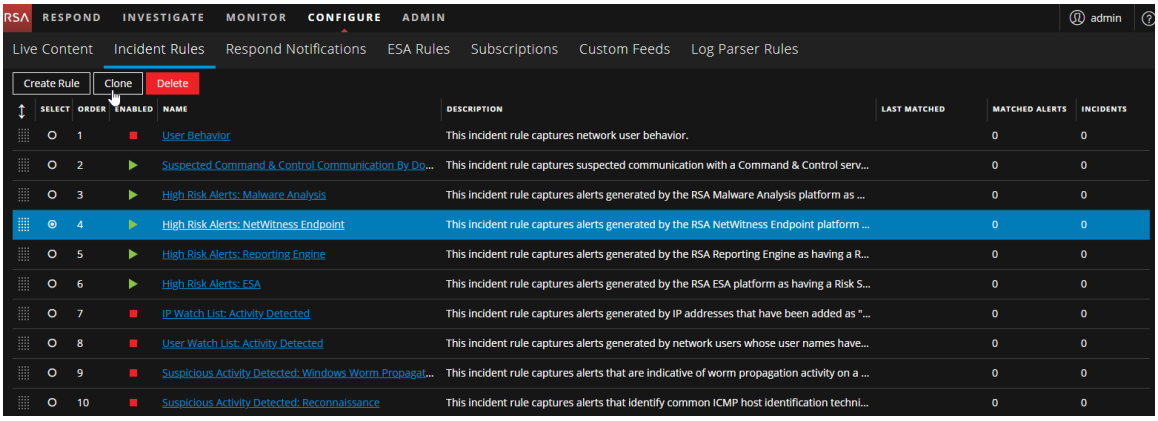
The following table shows the values for the Web Threat Detection default incident rule.

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}

Create a NetWitness Endpoint Incident Rule using Detector IP

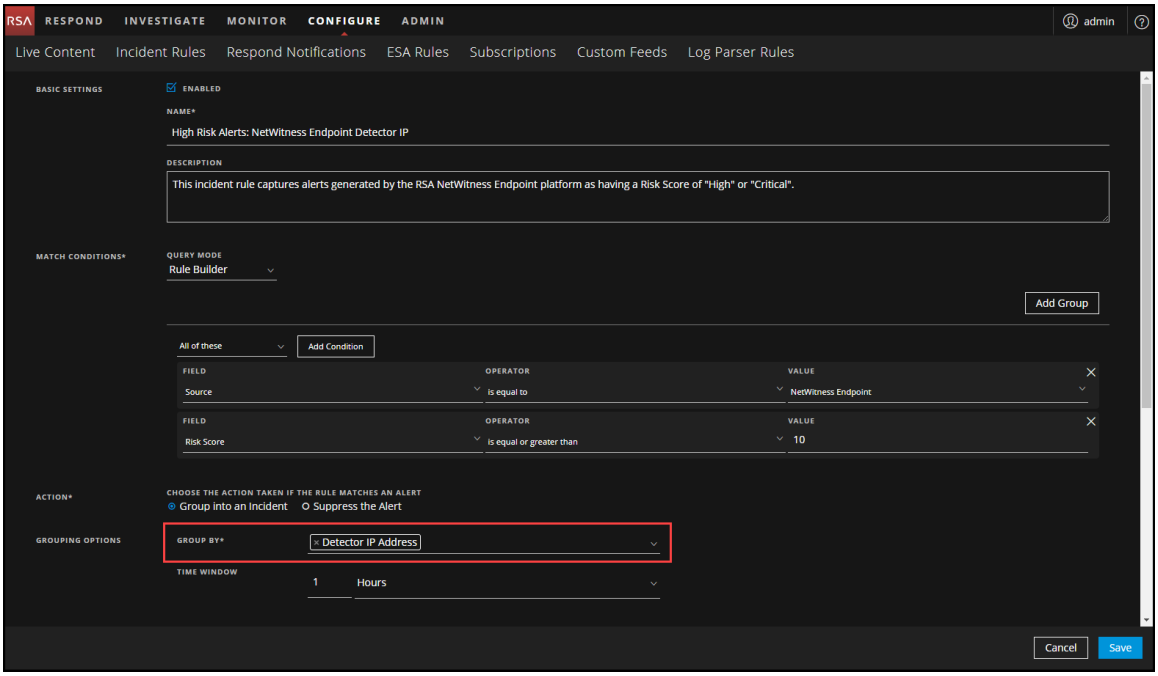
To aggregate NetWitness Endpoint alerts based on the Detector IP Address, create another NetWitness Endpoint Rule using the Detector IP Address as the Group By value. To do this, you clone the default NetWitness Endpoint incident rule and change the Group By IP address.

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

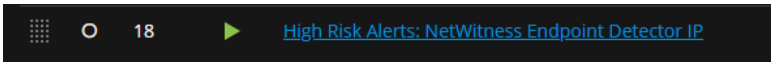


   You will receive a message that you successfully cloned the selected rule.
3. Change the **Name** of the rule to an appropriate name, such as High Risk Alerts: NetWitness Endpoint Detector IP.

4. In the **Group By** field, remove **Source IP Address** and add **Detector IP Address**.
   It is important that Detector IP Address is the only Group By value listed.



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

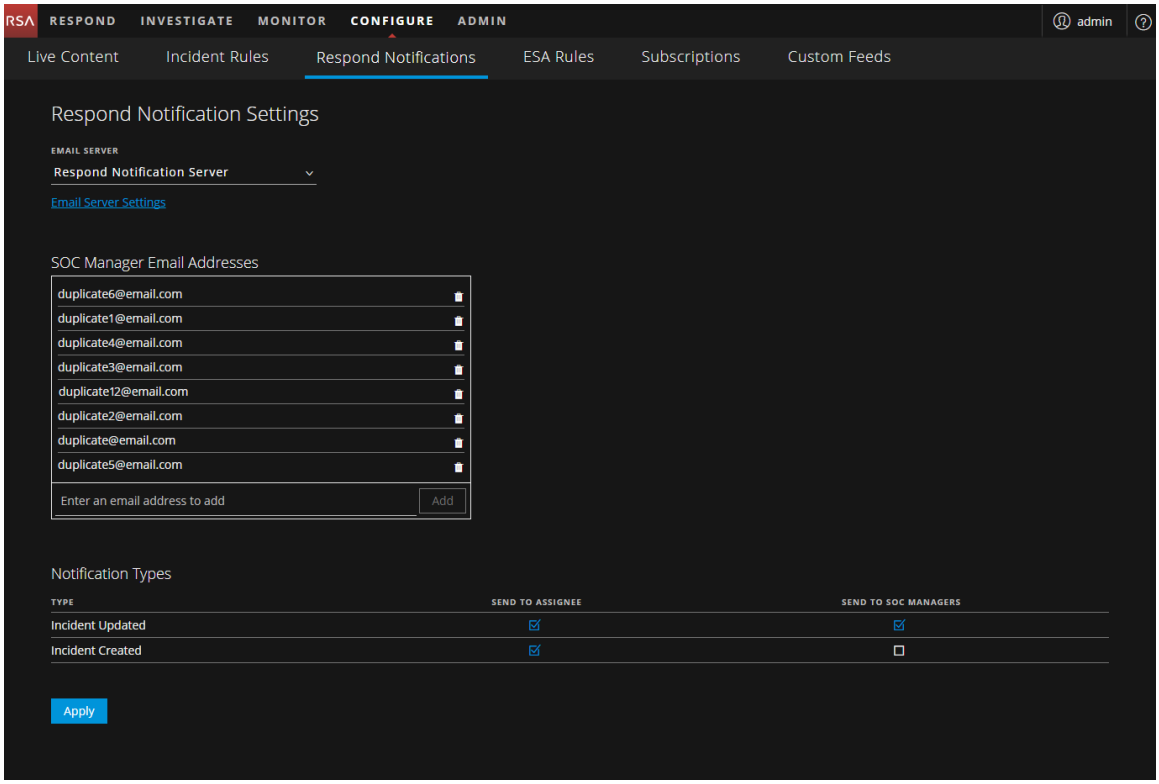


7. Verify the order of your incident rules. For more information, see Verify the Order of your Incident Rules .

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.



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.

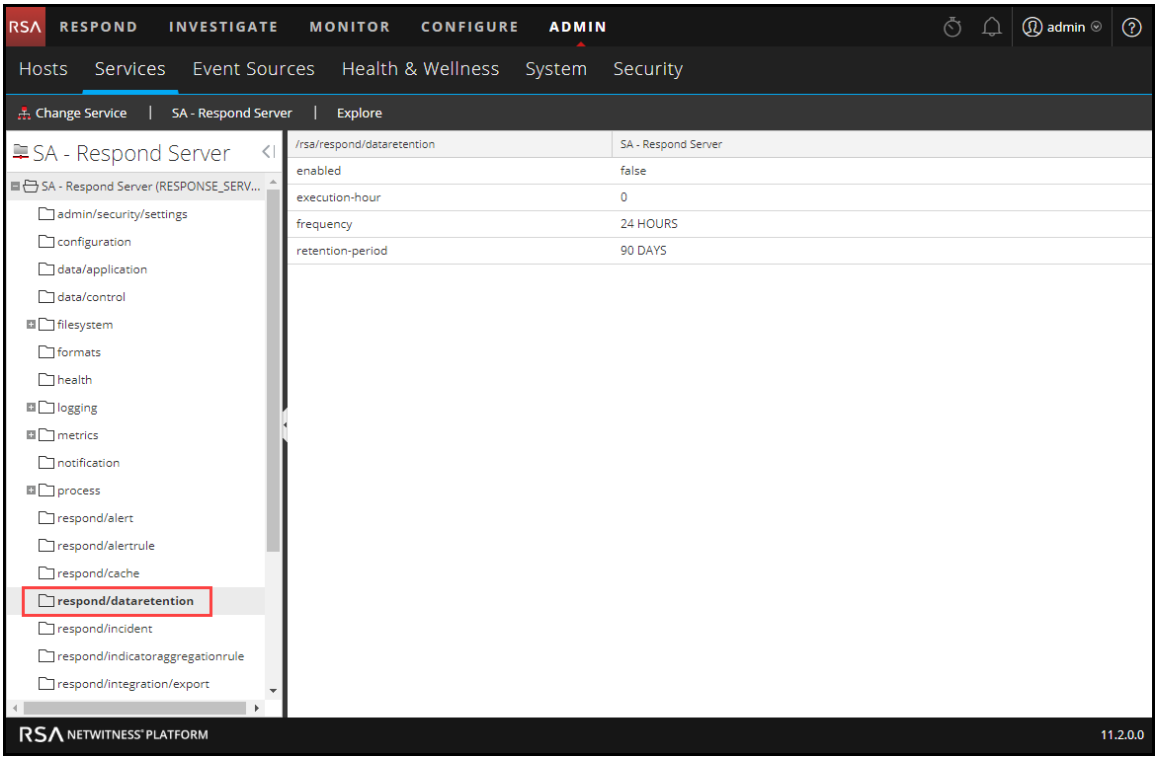
Prerequisites

The Administrator role must be assigned to you.

Procedure

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

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



3. 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.
4. 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.
   You will see a notice 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.

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.

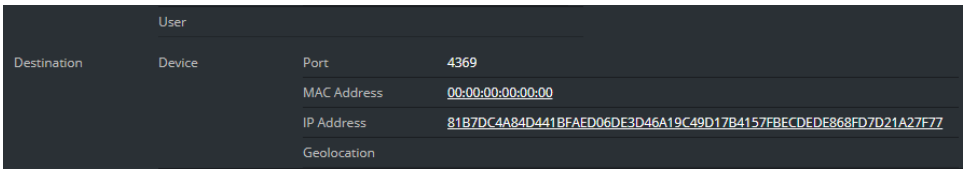
Procedure

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:



   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

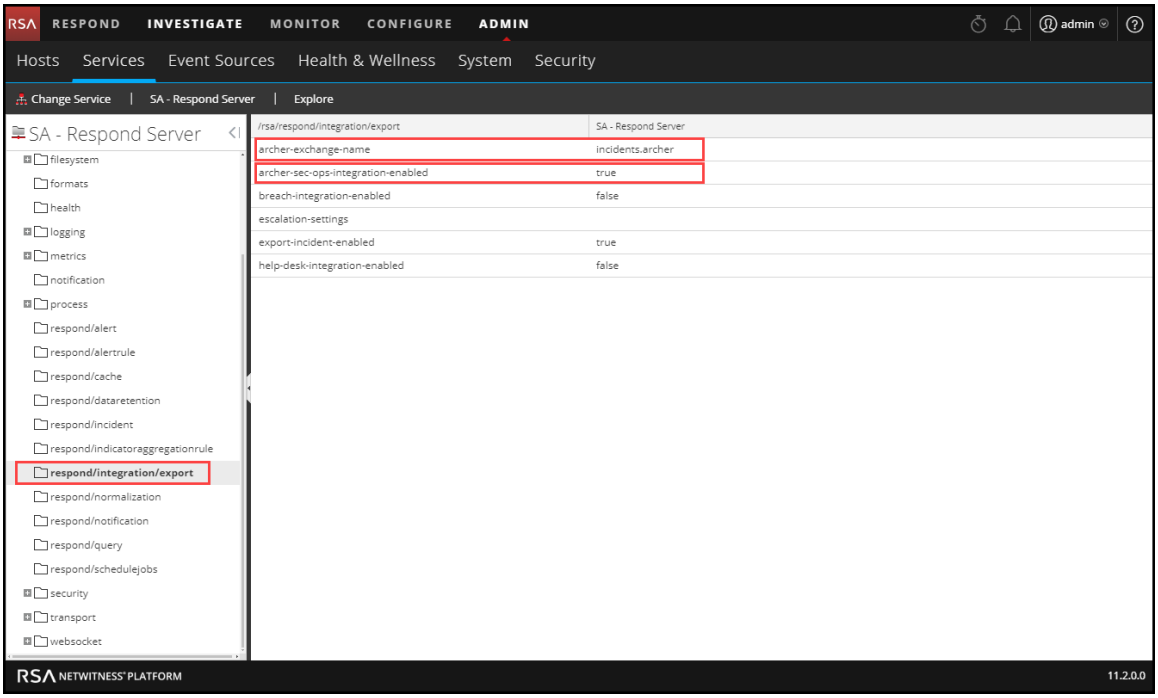
- Archer Cyber Incident & Breach Response 1.3.1.2 (NetWitness Platform 11.0 will only work with Archer Cyber Incident & Breach Response 1.3.1.2.)

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**.
   You will see a notice 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**.

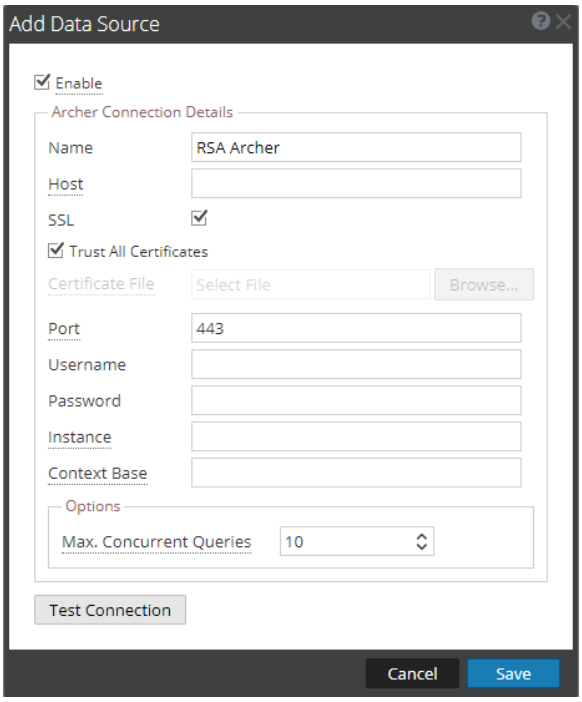
   The Services view is displayed.

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.



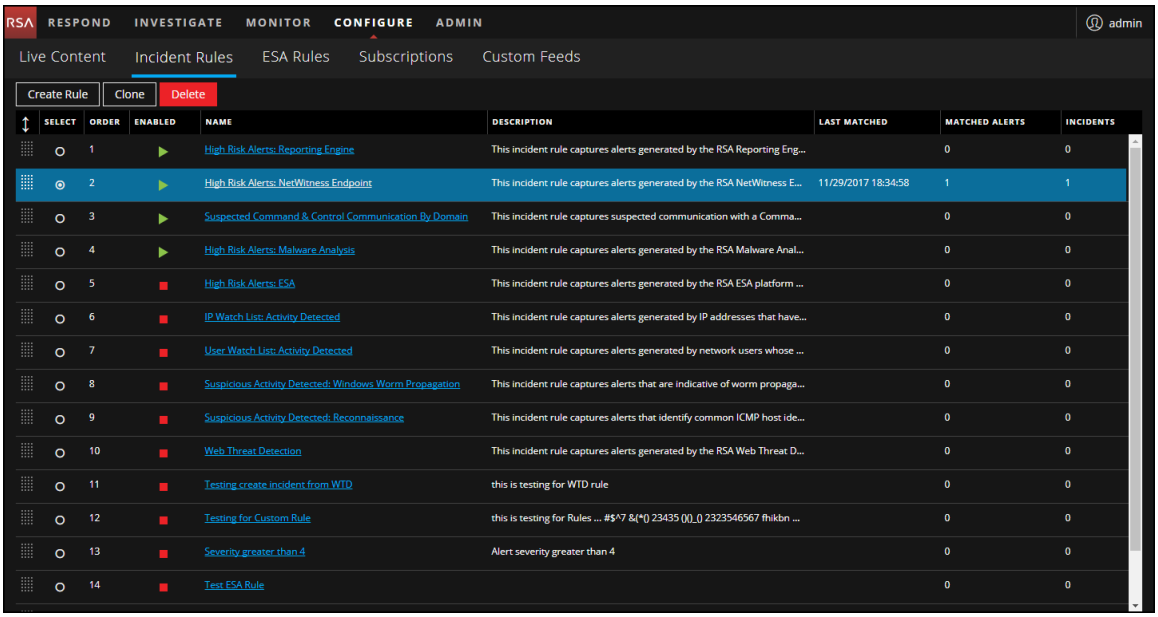
4. Provide the following information:

- 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 set up that includes unique content in a database, the connection to the database, the interface, and log-in. 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/**rsaarche**r/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. You will be able to see a Send to Archer button and Sent to Archer status in NetWitness Respond.

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 List view displays these counts in columns on the right.



These columns provide the following information for a rule:

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

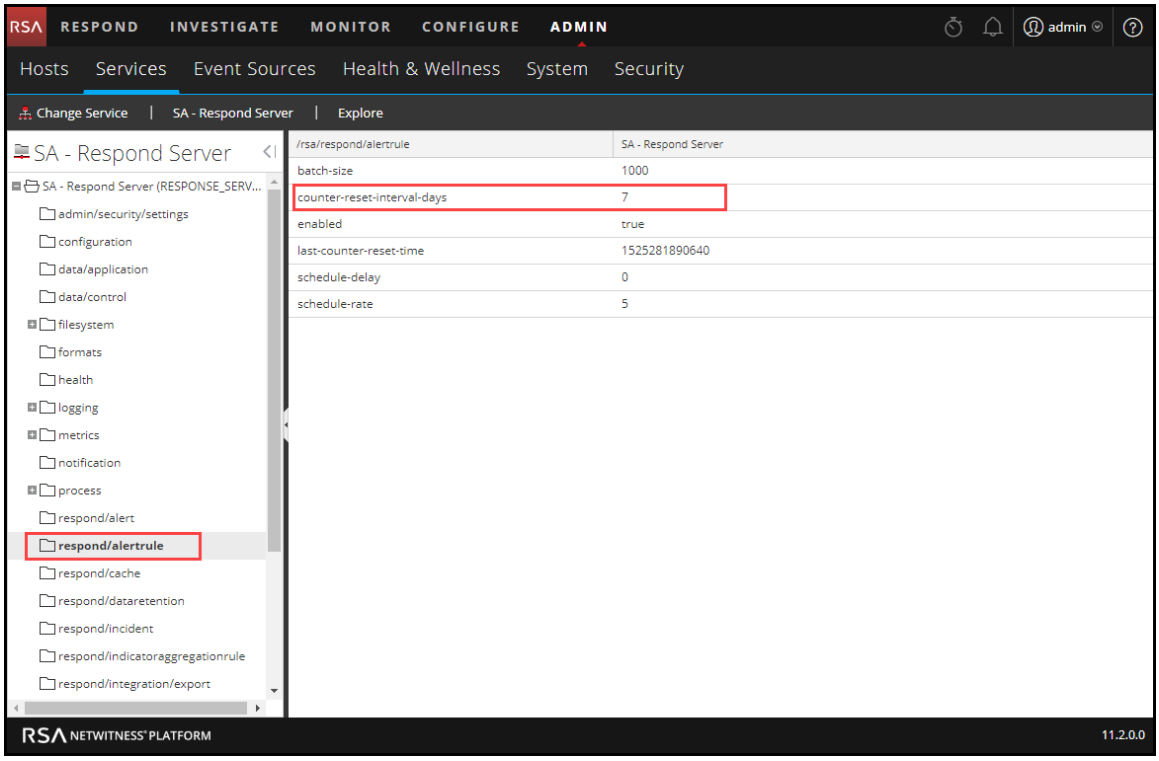
By default, these values reset to zero every 7 days. Depending on how long you want the counts to continue, you can change the default number of days.

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

To set a counter for matched alerts and incidents:

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

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



3. In the right panel, type the number of days in the **counter-reset-interval-days** field.
4. 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

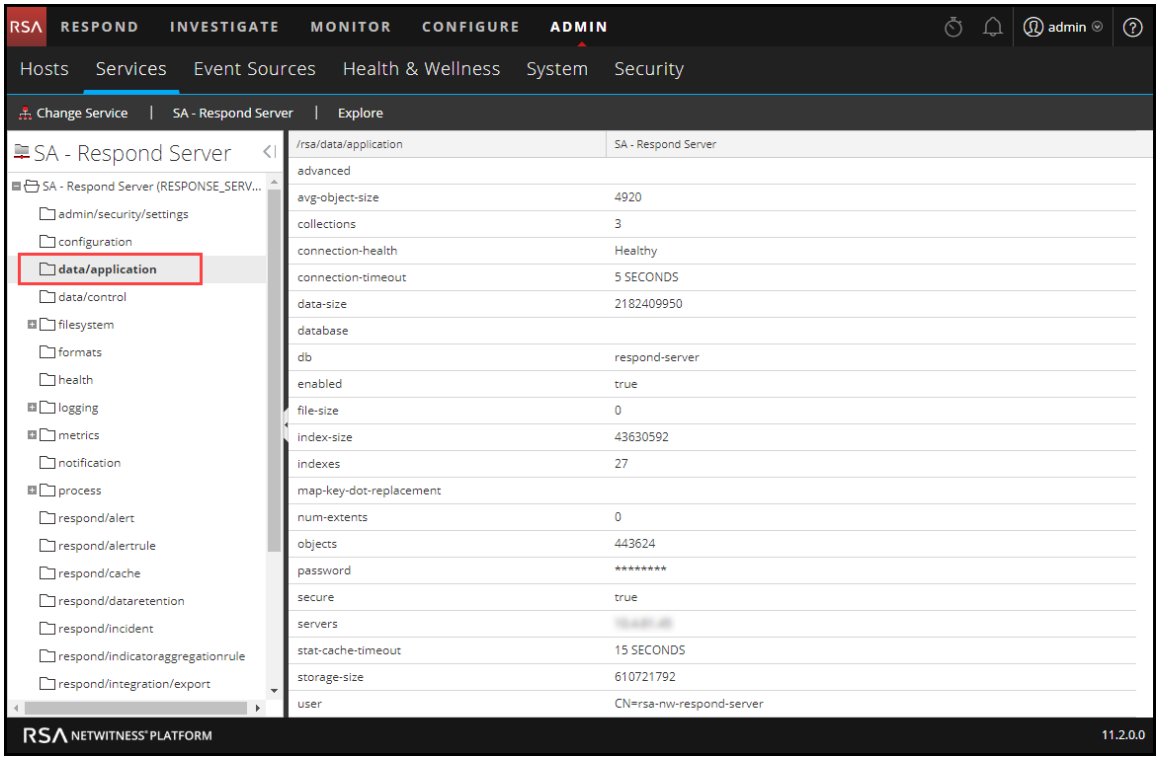
Ensure that:

- You have installed a host on which you want to run the Respond Server service. Refer to "Step 1: Deploy a Host" in the *Hosts and Services Getting Started Guide* for the procedure to add a host.
- The Respond Server service is installed and running on NetWitness Platform.
- An ESA host is installed and configured.

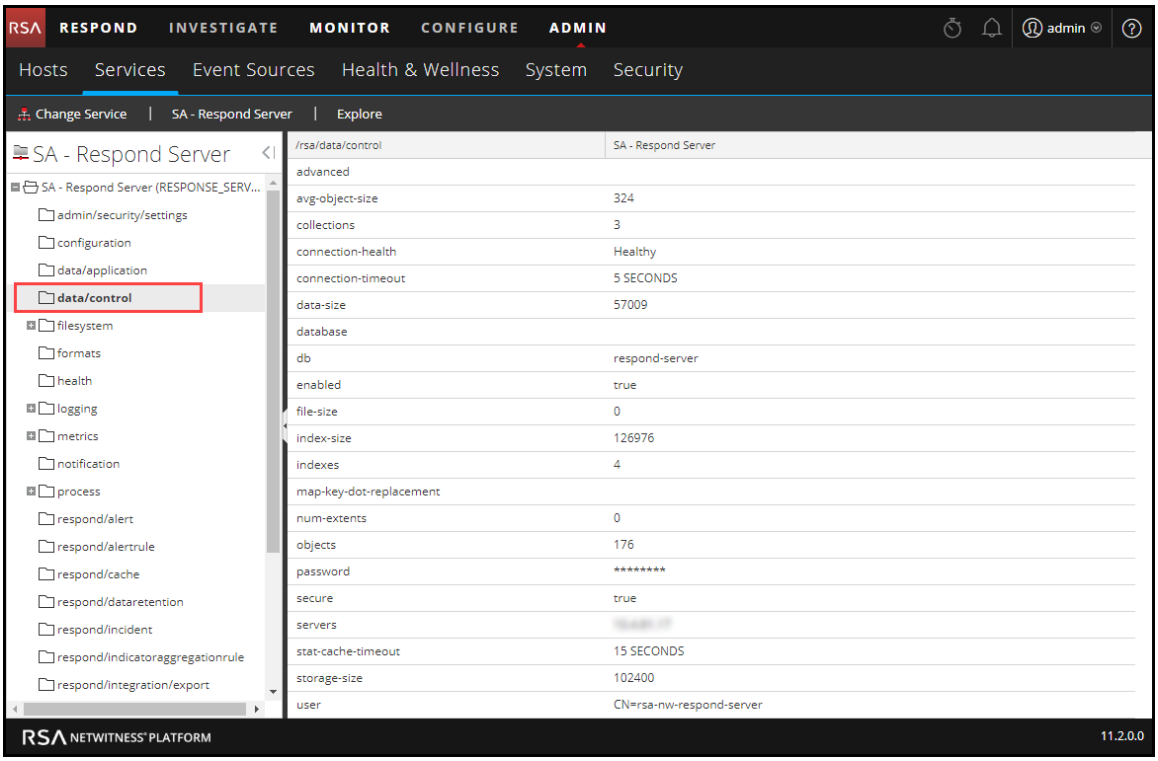
Procedure

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 List View

The Incident Rules List View 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.

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

What do you want to do?

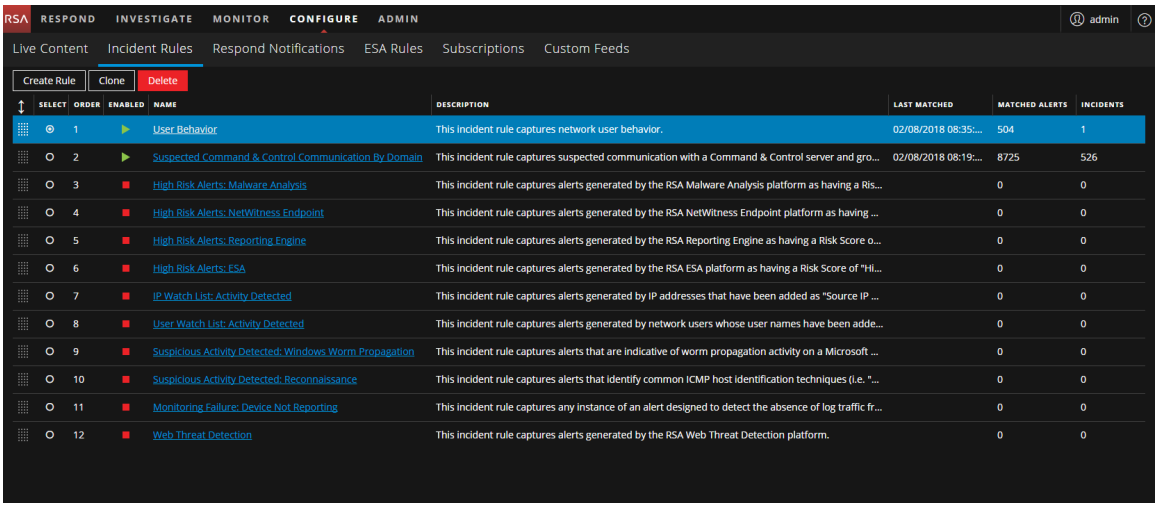
Role	I want to ...	Show me how
Analyst, Content Expert, SOC Manager	Create or edit an incident rule.	Step 3. Enable and Create Incident Rules for Alerts
Incident Responders, Analysts, Content Experts, SOC Manager	View the results of my incident rule (View Detected Threats).	See "Responding to Incidents" in the *NetWitness Respond User Guide*.

Related Topics

- Incident Rule Details View

Quick Look

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



The Incident Rules List view consists of a list and series of buttons.

Incident Rules List

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 two rules match an alert, only the rule with the highest priority is evaluated.
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 Set Counter for Matched Alerts and Incidents.
Incidents	Displays the number of incidents created by the rule. This value is reset once a week. To change the setting, see the Set Counter for Matched Alerts and Incidents.

Incident Rules Actions

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

Action	Description
Create Rule button	Allows you to add a new rule.
Delete button	Allows you to delete a rule.
Clone button	Allows you to duplicate a rule.
Name 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.	Step 3. Enable and Create Incident Rules for Alerts
Analyst, Content Expert, SOC Manager	Set up and use the User Behavior default rule. Set up or verify the preconfigured (default) incident rules.	Set Up and Verify Default Incident Rules
Incident Responders, Analysts, Content Experts, SOC Manager	View the results of my incident rule (View Detected Threats).	See "Responding to Incidents" in the *NetWitness Respond User Guide*.

Related Topics

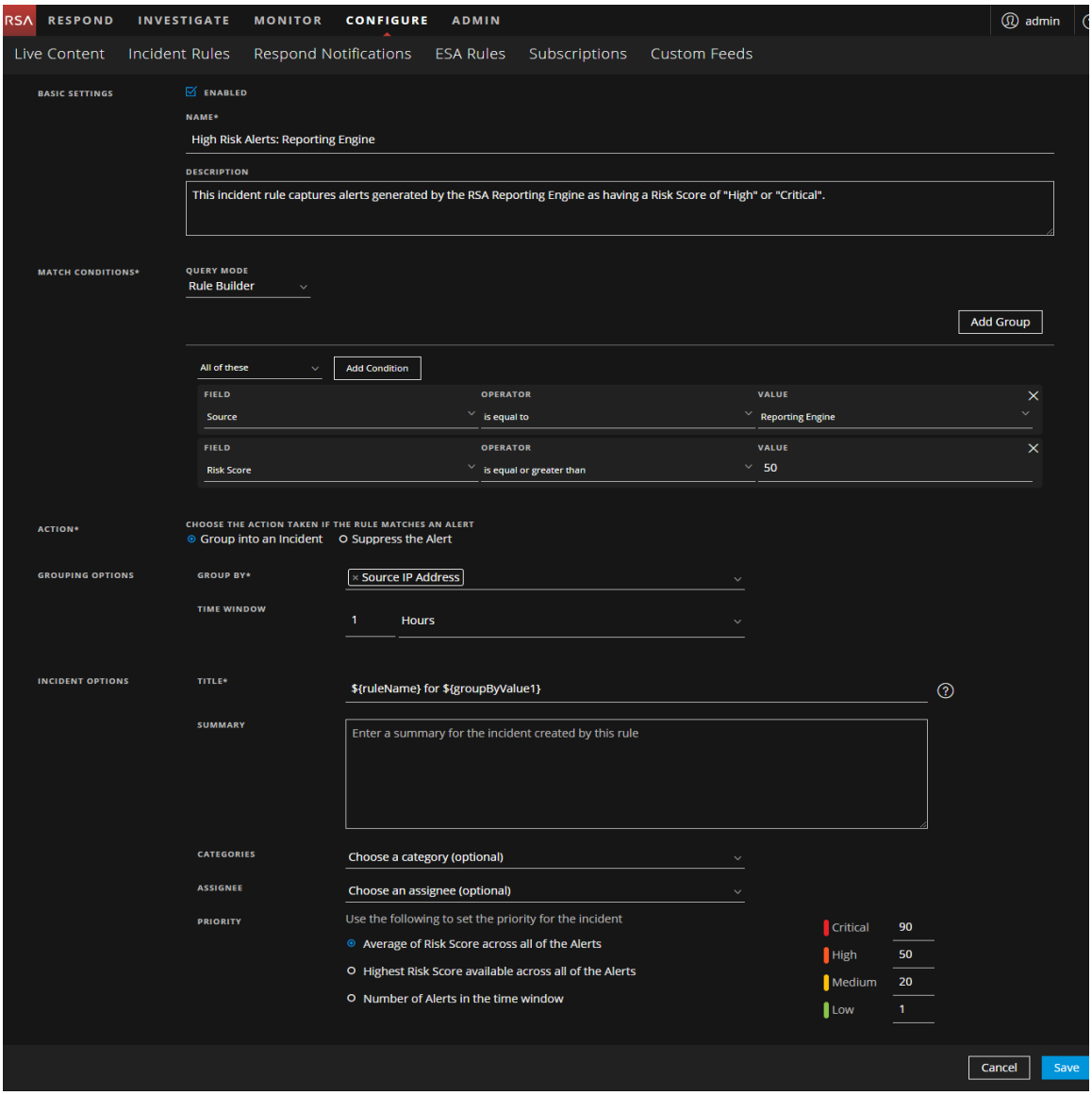
- Incident Rules List View

Quick Look

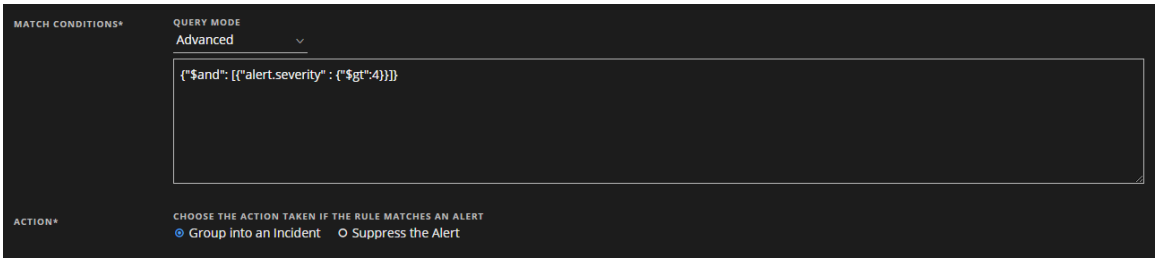
To access the Incident Rule Details view, do one of the following:

- 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 SET-TINGS	ENABLED	Select to enable the rule.
	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	**Rule Builder**: 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. In the Match Conditions, you can set the value to **All of these**, **Any of these**, or **None of these**. Depending on what you select, the criteria types specified in the Conditions and Group of conditions are matched to group the alerts. For example, if you set the match condition to **All of these**, alerts that match the criteria mentioned in the Conditions and Group Conditions are grouped into one incident. • Add a Condition to be matched by clicking the **Add Condition** button. • Add a Group of Conditions by clicking the **Add Group** button and add conditions by clicking the **Add Condition** button. You can include multiple Conditions and Groups of Conditions that can be matched as per criteria set and group the incoming alerts into incidents. **Advanced**: Select 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. For example, you can type the criteria builder format **{"$and": [{"alert.severity" : {"$gt":4}}]}** to group alerts that have severity greater than 4. For advanced syntax, refer to http://docs.mongodb.org/manual/reference/operator/query/ or http://docs.mongodb.org/manual/reference/method/db.collection.find/

Section	Field	Description
ACTION*	CHOOSE THE ACTION TAKEN IF THE RULE MATCHES THE ALERT	**Group into an Incident**: If enabled, the alerts that match the criteria set are grouped into an alert. **Suppress the Alert**: If enabled, the alerts that match the criteria are suppressed.
GROUPING OPTIONS	GROUP 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 **Group By Meta Key Mappings** table.)
	TIME WINDOW	The time range for grouping alerts. 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*	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. For example, if you grouped them according to the source, you can name the resulting Incident as Alerts for **${groupByValue1}**, and the incident for all alerts from NetWitness Endpoint would be named **Alerts for NetWitness Endpoint**.
	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	**Average of Risk Score across all of the Alerts**: Takes the average of the risk scores across all the alerts to set the priority of the incident created. **Highest Risk Score available across all of the Alerts**: Takes the highest score available across all the alerts to set the priority of the incident created. **Number of Alerts in the time window**: Takes the count of the number of alerts in the time window selected to set the priority of the incident created. **Critical, High, Medium, and Low**: Specify the incident priority threshold of the matched incidents. The defaults are: • Critical: 90 • High: 50 • Medium: 20 • Low: 1 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.

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

Group By Field Value	Mapped Meta Key
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 Version 11.1 and later.

What do you want to do?

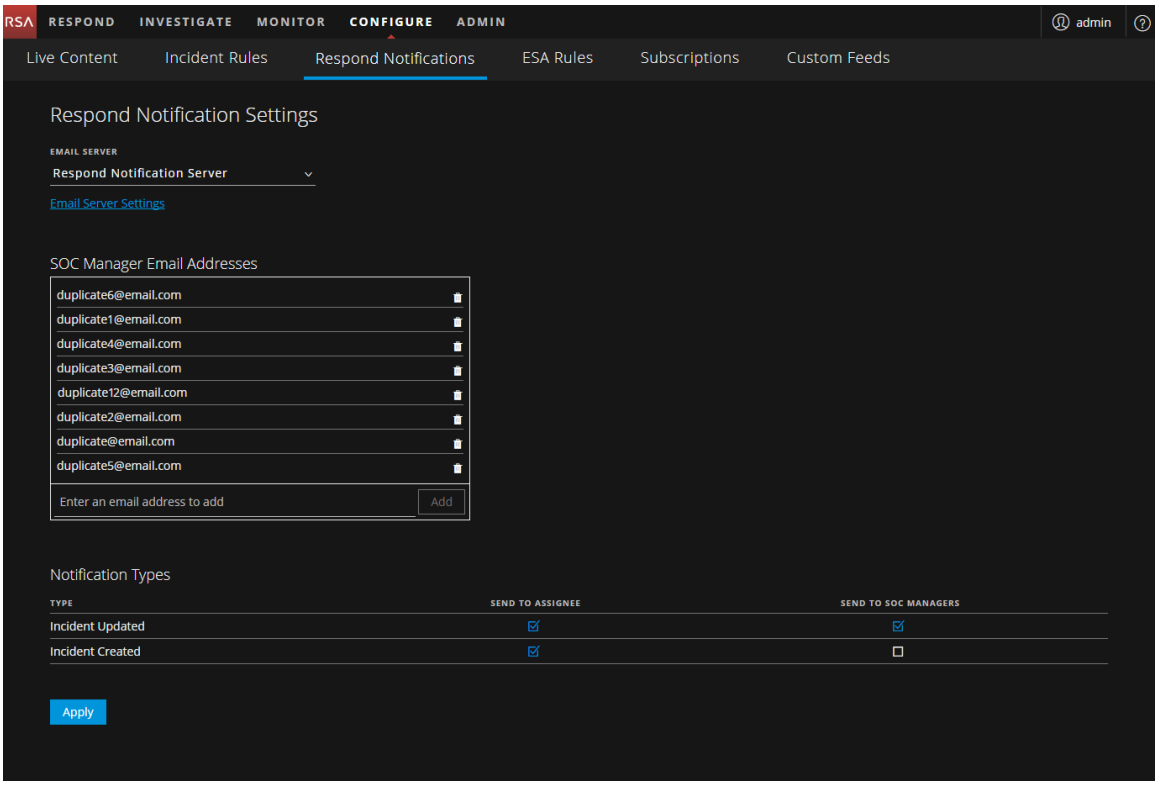
Role	I want to ...	Show me how
Administrator	Configure an email server.	Refer to "Configure the Email Settings as Notification Server" in the *System Configuration Guide*. (To access these settings, click the **Email Server Settings** link or go to ADMIN > System > Global Notifications > Servers tab.)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

Related Topics

- Incident Rules List 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. Clicking the **Email Server Settings** link goes to ADMIN > SYSTEM > Global Notifications. For instructions, refer to "Configure the Email Settings as Notification Server" in the *System Configuration Guide*.
SOC Manager Email Addresses	Lists the SOC Manager email addresses that receive email notifications when you select **Send to SOC Manager** 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. • **Send to Assignee**: When an incident is created, an email is sent to the Analyst assigned to the incident. • **Send to SOC Manager**: When an incident is created, an email is sent to all of the addresses listed in the SOC Manager Email Addresses list.

Setting	Description
Notification Types - Incident Updated	Specifies who should receive an email notification when an incident is created. • **Send to Assignee**: When an incident is updated, an email is sent to the Analyst assigned to the incident. • **Send to SOC Manager**: When an incident is updated, an email is sent to all of the addresses listed in the SOC Manager Email Addresses list.
Apply	Applies changes made to Respond Notification Settings. Changes to these settings 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.

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?

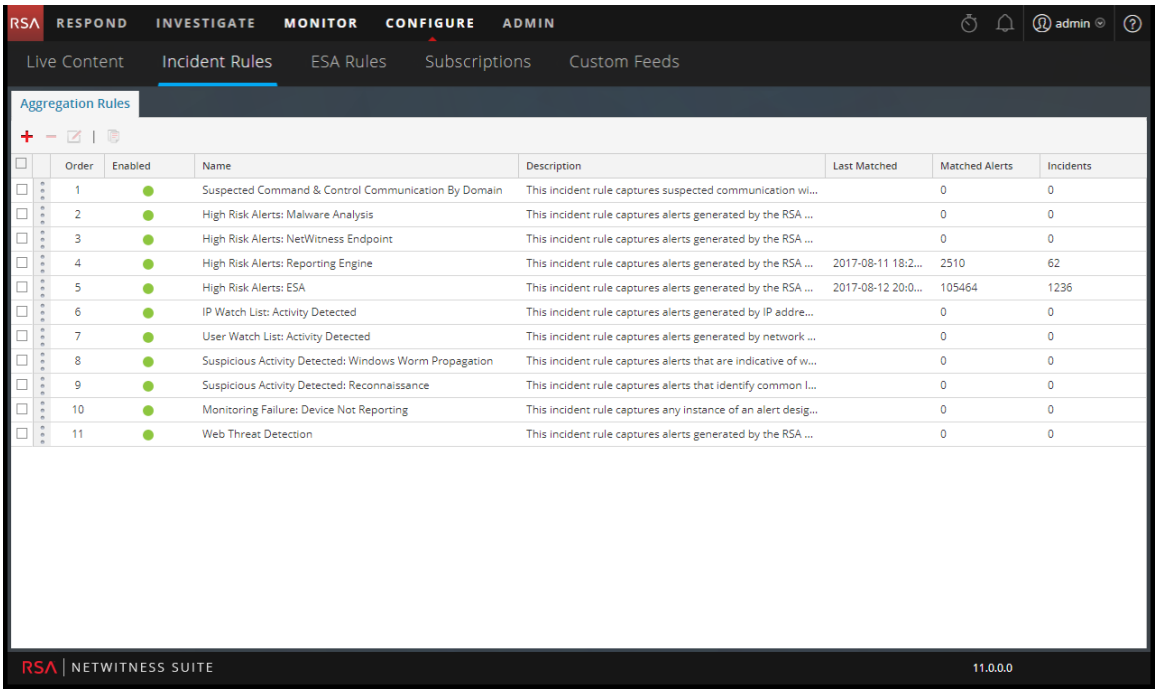
Role	I want to ...	Show me how
Analyst, Content Expert, SOC Manager	Create an aggregation rule.	Step 3. Enable and Create Incident Rules for Alerts
Incident Responders, Analysts, Content Experts, SOC Manager	View the results of my aggregation rule (View Detected Threats).	See "Responding to Incidents"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

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.

Column	Description
Matched Alerts	Displays the number of matched alerts. This value is reset once a week. To change the setting, see Set Counter for Matched Alerts and Incidents.
Incidents	Displays the number of incidents created by the rule. This value is reset once a week. To change the setting, see the Set Counter for Matched Alerts and Incidents.

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.	Step 3. Enable and Create Incident Rules for Alerts
Incident Responders, Analysts, Content Experts, SOC Manager	View the results of my aggregation rule (View Detected Threats).	See "Responding to Incidents" in the *NetWitness Respond User Guide*.

Related Topics

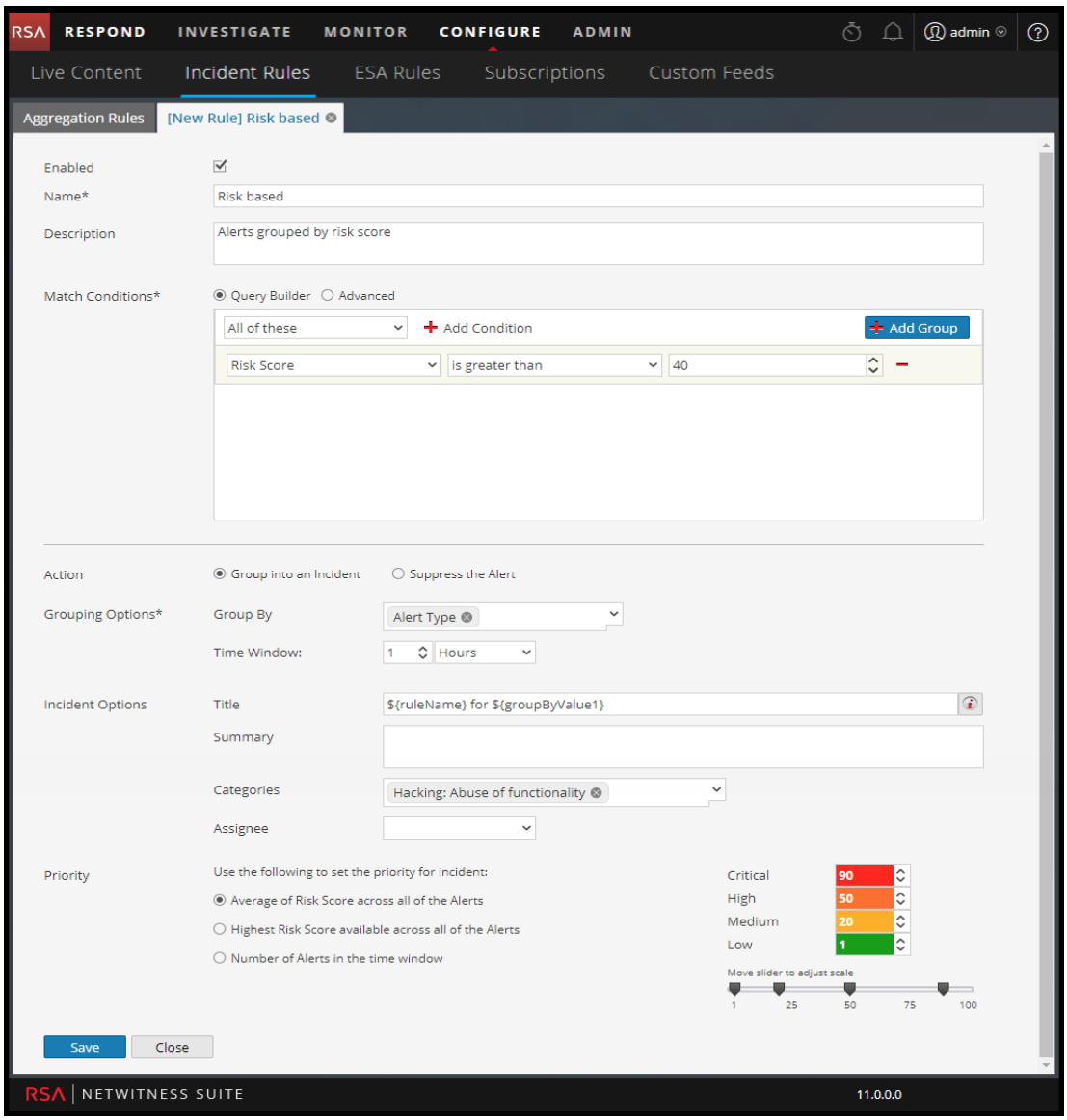
- Aggregation Rules Tab

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*	**Query Builder** - Select if you want to build a query with various conditions that can be grouped. You can also have nested groups of conditions. Match Conditions - You can set the value to **All of these**, **Any of these**, or **None of these**. Depending on what you select, the criteria types specified in the Conditions and Group of conditions are matched to group the alerts. **For example**, if you set the match condition to **All of these**, alerts that match the criteria mentioned in the Conditions and Group Conditions are grouped into one incident. • Add a Condition to be matched by clicking + **Add Condition**. • Add a Group of Conditions by clicking + **Add Group** and adding conditions by clicking + **Add Condition**. You can include multiple Conditions and Groups of Conditions that can be matched as per criteria set and group the incoming alerts into incidents.
	Advanced - Select if you want to add an advanced query builder. You can add a specific condition that needs to be matched as per the matching option selected. **For example:** you can type the criteria builder format **{"$and": [{"alert.severity" : {"$gt":4}}]}** to group alerts that have severity greater than 4. For advanced syntax, refer to http://docs.mongodb.org/manual/reference/operator/query/ or http://docs.mongodb.org/manual/reference/method/db.collection.find/
Action	**Group into an Incident** - If enabled, the alerts that match the criteria set are grouped into an alert. **Suppress the Alert** - If enabled, the alerts that match the criteria are suppressed.
Grouping Options*	**Group By:** 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). Grouping on an attribute means that all matching Alerts containing the same value for that attribute are grouped together in the same incident. **Time Window:** The time range specified to group alerts. For example if the time window is set to 1 hour, all alerts that match the criteria set in Group By field and that arrive within an hour of each other are grouped into an incident.

Field	Description
Incident Options	**Title -** (Optional) Title of the incident. You can provide placeholders based on the attributes you grouped. Placeholders are optional. If you do not use placeholders, all Incidents created by the rule will have the same title. For example, if you grouped them according to the source, you can name the resulting Incident as Alerts for **${groupByValue1}**, and the incident for all alerts from NetWitness Endpoint would be named **Alerts for NetWitness Endpoint**.
	Summary - (Optional) Summary of the incident.
	Category - (Optional) Category of the incident created. An incident can be classified using more than one category.
	Assignee - (Optional) Name of the assignee to whom the incident is assigned to.
Priority	**Average of Risk Score across all of the Alerts** - Takes the average of the risk scores across all the alerts to set the priority of the incident created. **Highest Risk Score available across all of the Alerts** - Takes the highest score available across all the alerts to set the priority of the incident created. **Number of Alerts in the time window** - Takes the count of the number of alerts in the time window selected to set the priority of the incident created. **Critical, High, Medium, and Low** - Specify the incident priority threshold of the matched incidents. The defaults are: • Critical: 90 • High: 50 • Medium: 20 • Low: 1 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. You can change these defaults by manually changing the priorities or by moving the slider under **Move slider to adjust scale**.