NetWitness® Platform XDR

Version 12.0

NetWitness Respond Configuration

NETWITNESS
Platform XDR

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates 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 RSA.

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 NetWitness Community. 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

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

July, 2022

Contents

About this Document

The *NetWitness Respond Configuration Guide for NetWitness® Platform* provides an overview of NetWitness, 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

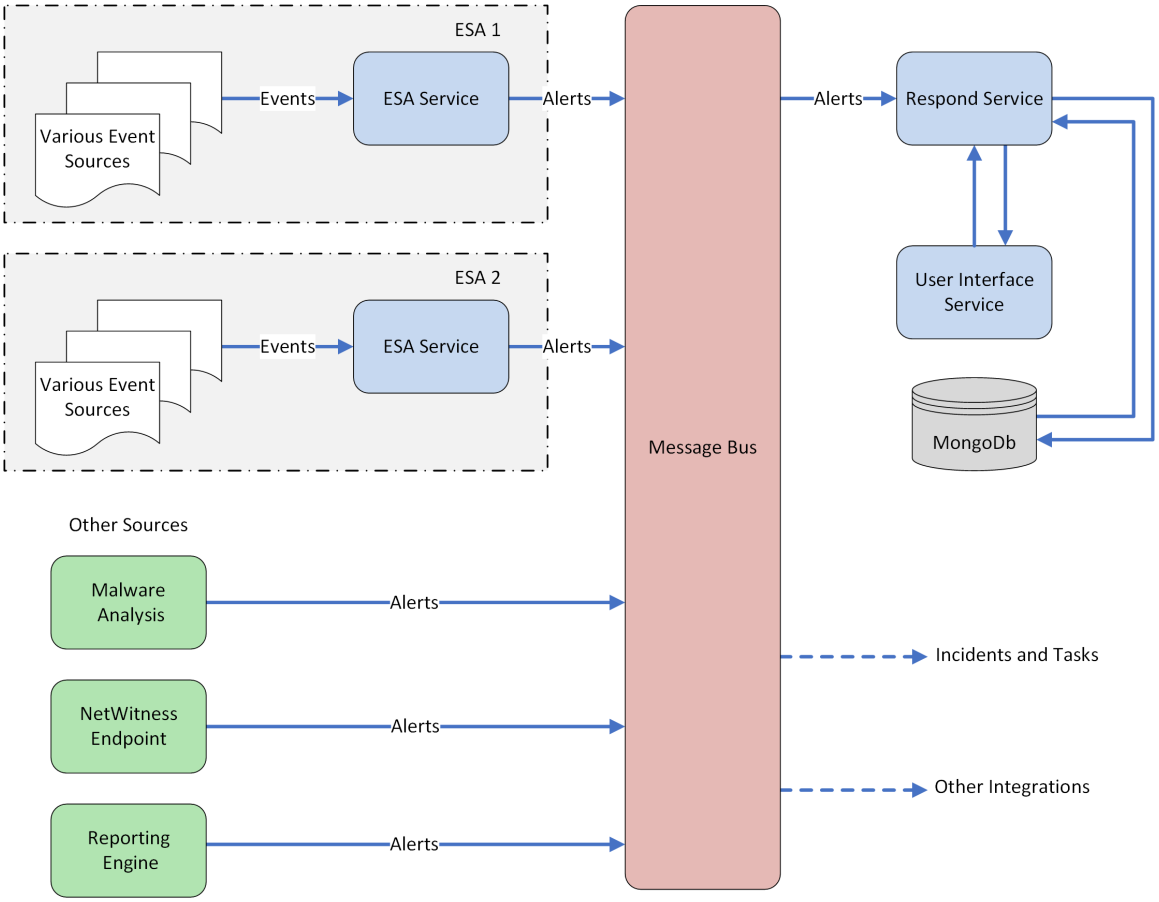
NetWitness Respond Configuration Overview

NetWitness Respond consumes alert data from various sources via the Message Bus and displays these alerts on the NetWitness 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 for Detect AI, Reporting Engine, Malware Analysis, and NetWitness Endpoint and enabled only for 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:

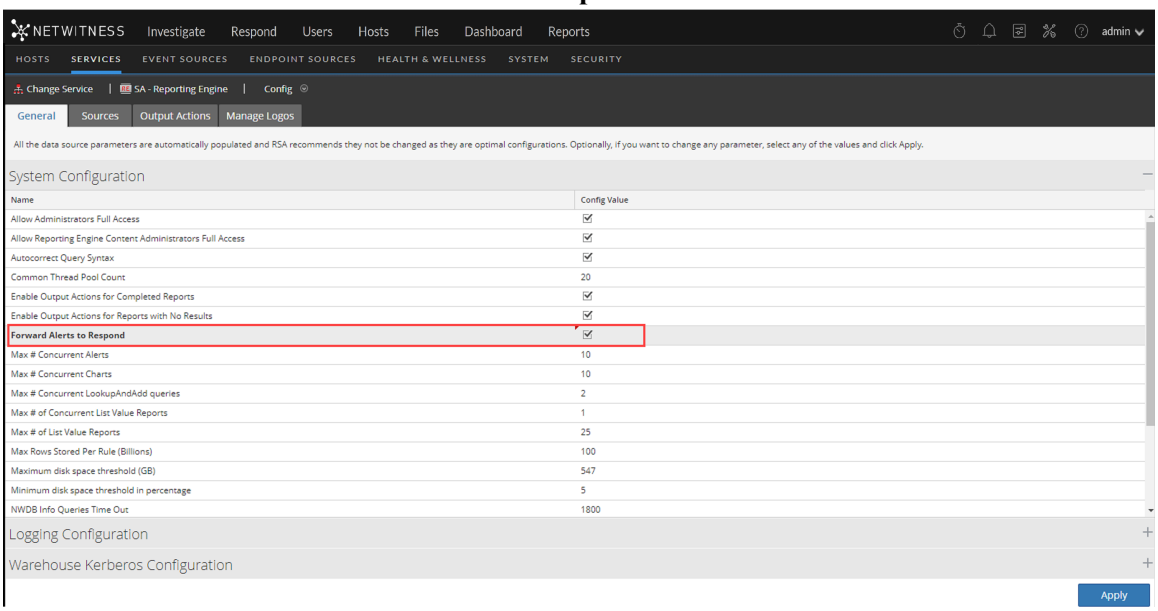
- The Respond Server service is installed and running on NetWitness.
- NetWitness Endpoint is installed and running. This is necessary only if you want to configure NetWitness Endpoint as an alert source in the Respond view.

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*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

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

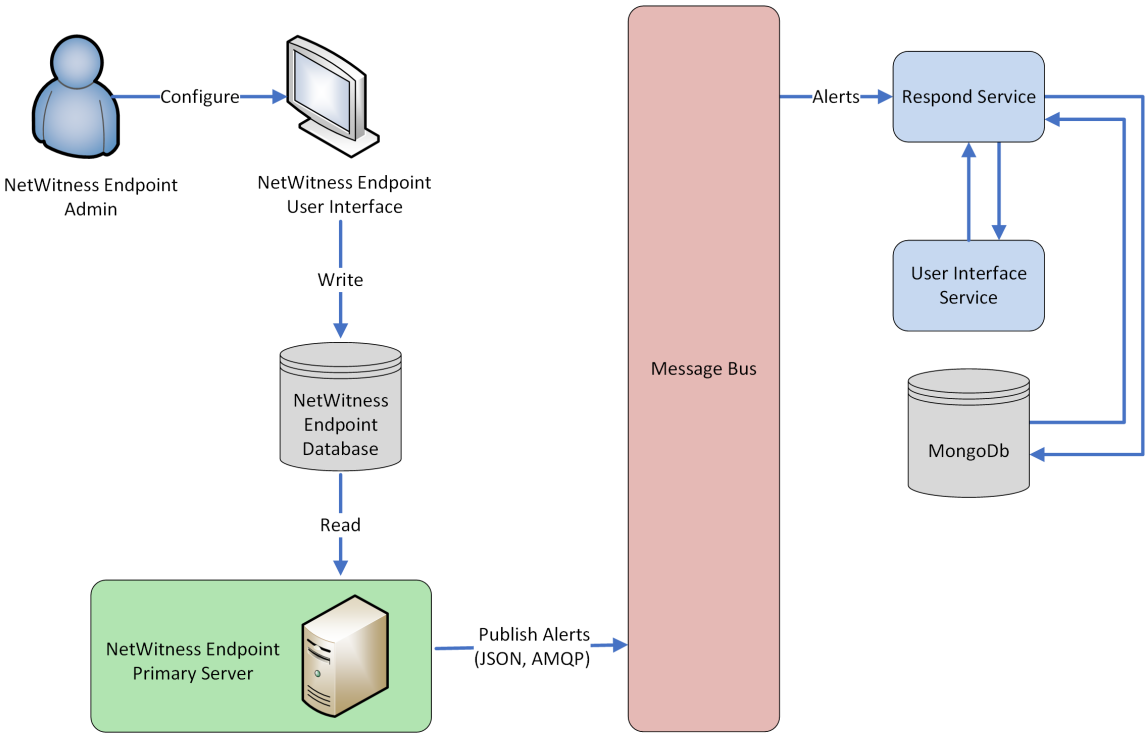
Viewing NetWitness Respond alerts is a function of auditing in Malware Analysis. The procedure for enabling NetWitness Respond alerts is described in the "(Optional) Configure Auditing on Malware Analysis Host" topic in the *Malware Analysis Configuration Guide*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

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

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

Note: NetWitness 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 "NetWitness Endpoint Integration" in the *NetWitness Endpoint User Guide*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

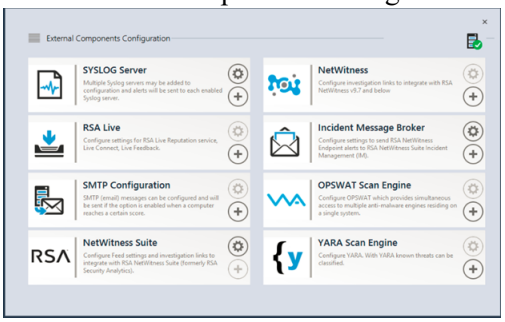
The diagram below represents the flow of NetWitness Endpoint alerts to the NetWitness Respond Server service and its display in the **Respond > Alerts** view.



To configure NetWitness Endpoint to display NetWitness Endpoint alerts in the NetWitness 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 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 incident email 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. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.
- **Respond_Administrator**: The Respond Administrator has full access to NetWitness Respond.
- **Administrators**: The Administrator has full system access to NetWitness 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 incident email 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
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 version 11.1 and later.

Users who configure incident email notification settings also need Integration-server permissions. The following table lists the incident notification 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

Incident Email Notification Settings Permissions

Note: Incident email notification setting permissions are available in NetWitness version 11.1 and later.
If you are updating from NetWitness version 11.0 to 11.1 or later, you will need to add additional permissions to your existing built-in NetWitness 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 incident email notification settings [ (Configure) > Incident 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 version 11.2 and later.

The Events panel in the Respond view, formerly known as the Event Analysis panel, shows the Events view from Investigate for specific indicator events. The following permissions are required to view the Events panel 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 versions before 11.2 will not show the Events 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 Events panel in the Respond view for those incidents.

Respond Saved Filter Permissions

Note: Saved filters for the incidents and alerts lists in Respond are available in NetWitness version 11.5 and later.

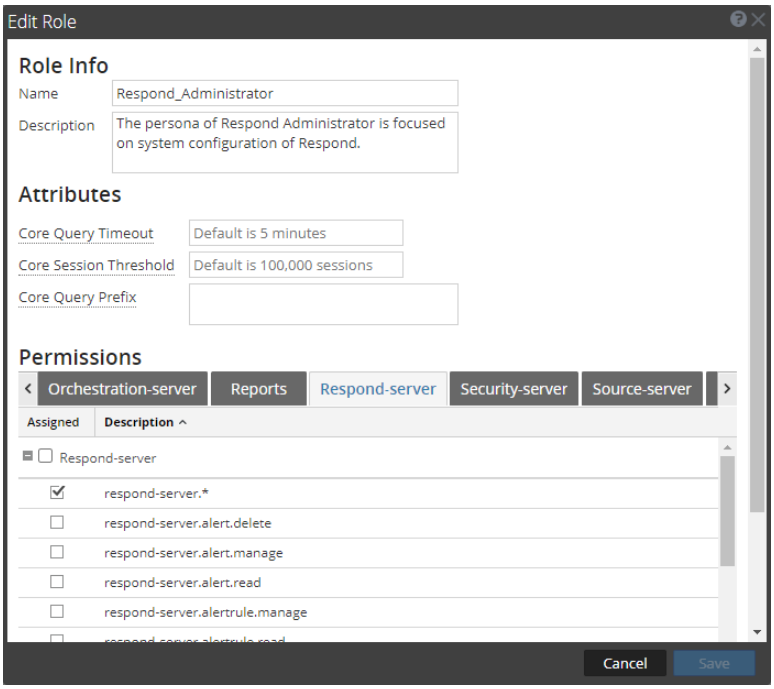
The following permissions are required for the incidents and alerts filters (Respond > Incidents and Respond > Alerts). The Analysts role has the required Respond filter permissions by default.

Respond-server tab:

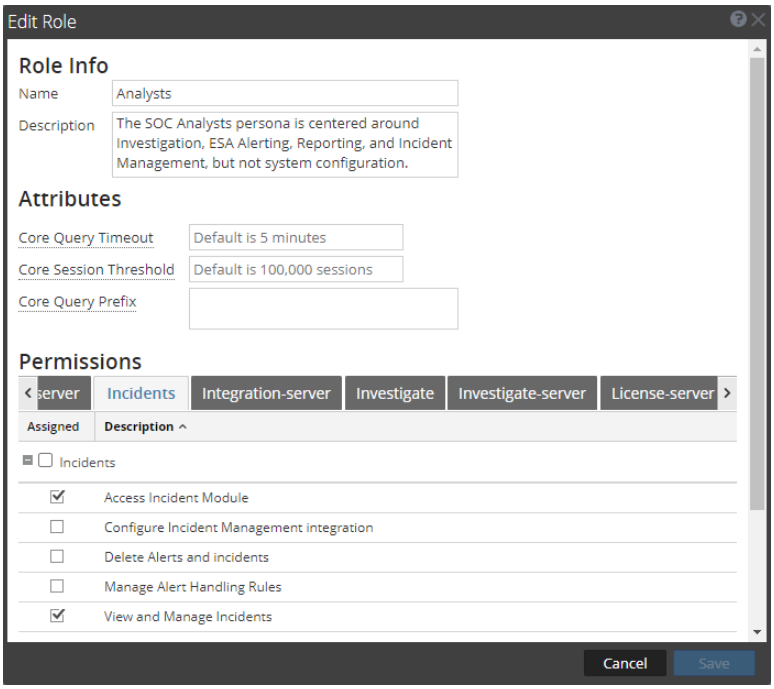
- respond-server.incident.manage
- respond-server.incident.read
- respond-server.alert.manage
- respond-server.alert.read

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*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Restrict Access to Incidents

By default, analysts can view all of the incidents, alerts, and tasks in the Respond view. If you have sensitive or restricted information that should not be shared, you can restrict what analysts and other users can see in the Respond view.

If you restrict access to incidents:

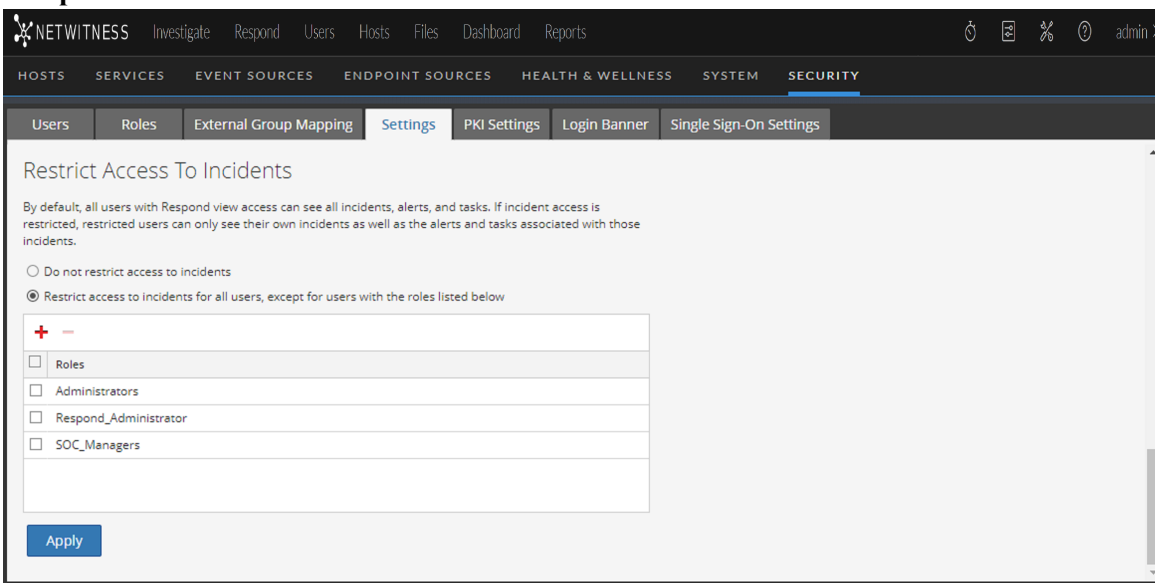
- Analysts can only see incidents assigned to them as well as the alerts and tasks associated with those incidents. Likewise, they can only change the status of and add journal entries (notes) to their own incidents.
- Analysts cannot see the Alerts and Tasks tabs in the Respond view (Respond > Tasks and Respond > Alerts are hidden), so they cannot view all alerts and tasks.
- Analysts cannot see the Assignee button or change the assignee of an incident.
- Analysts cannot see the Related Indicators (alerts) panel (Incident Details view > Find Related tab in the left-side panel).
- When adding events to incidents from the Investigate views, users can only add events to incidents to which they have access. The list of incidents to which users can add events only shows incidents that the user can access.

- When creating incidents from the Investigate views, users must have access to those incidents to view them in the Respond view. For example, when creating incidents from the Investigate view, Analysts must assign the incidents to themselves to view them in the Respond view.

Caution: These restrictions apply to all NetWitness users, except users with the **Administrators**, **Respond_Administrator**, and **SOC_Managers** roles. However, you can adjust the list of user roles whose access to incidents should not be restricted.

To restrict access to incidents:

1. Go to  **(Admin) > Security** and click the **Settings** tab.
2. In the **Restrict Access to Incidents** section, select **Restrict access to incidents for all users, except for users with the roles listed below**.



3. In the list, add the user roles whose access to incidents should not be restricted.
4. Click **Apply**.
   Changes take effect on the next log in to NetWitness.

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 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.

In 11.6.1, the Incident rule execution pattern is modified such that the alert aggregation queries refer to the lastRun parameter of the incident rule. So, now multiple incident rules (positioned as per the priority in the order field) in the Incident rules list match the same alert name.

For example,

- INC-rule 1 is at the 4th position in the order field that is associated with the conditions alert.name equal to test and **source** equal to **ESA**.
- INC-rule 2 is at the 24th position in the order field that is associated with the condition **source** equal to **ESA**.

  Before 11.6.1 upgrade, the INC-rule 1 matched the alert name test. On upgrade, the INC-rule 2 at the 24th position in the order field matches the alert name test as the source is ESA.

  To address this scenario, configure each incident rule to have unique conditions. Make sure the conditions in the lower priority incident rules are not duplicate of the conditions in the highest priority rules.

NetWitness 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
- Export and import rules

The Detect AI default incident rule is available in NetWitness 11.6 and later. It captures the network user behavior and uses the deployed RSA Live ESA Rules to create incidents from alerts.

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 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.

To configure the default incident rules or verify your existing default incident rules with the 11.5 default incident rules, see Set Up and Verify Default Incident Rules.

This topic contains the following procedures:

- Enable Incident Rules
- Create an Incident Rule
- Verify the Order of Your Incident Rules
- Clone an Incident Rule
- Edit an Incident Rule
- Export Incident Rules
- Import Incident Rules

Enable Incident Rules

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.

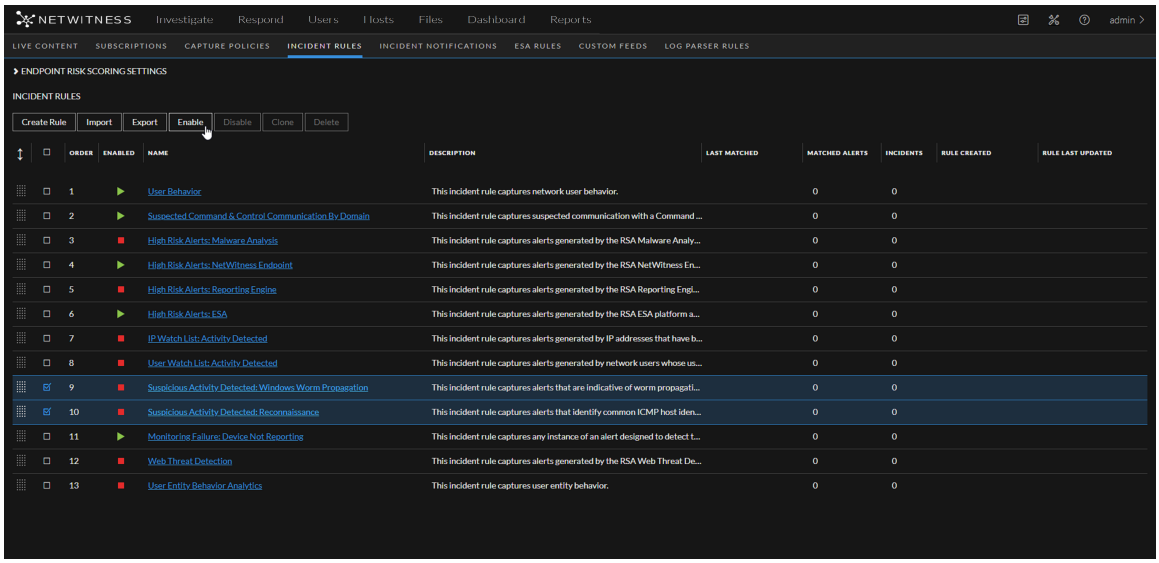
To enable one or more incident rules:

Note: Enabling one or more incident rules from the Incident Rules view is only available in NetWitness version 11.4 and later.

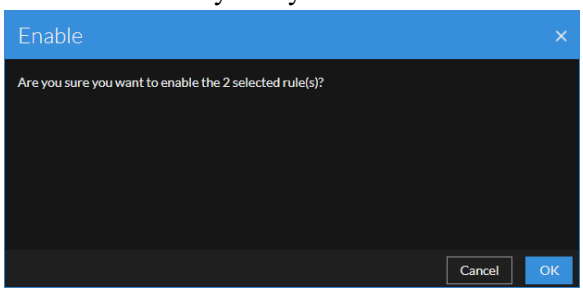
This is the easiest way to enable rules. Use this method after you have made the necessary adjustments to the rules and you just want to quickly enable them.

1. Go to  **(Configure) > Incident Rules**.
   The Incident Rules view is displayed.

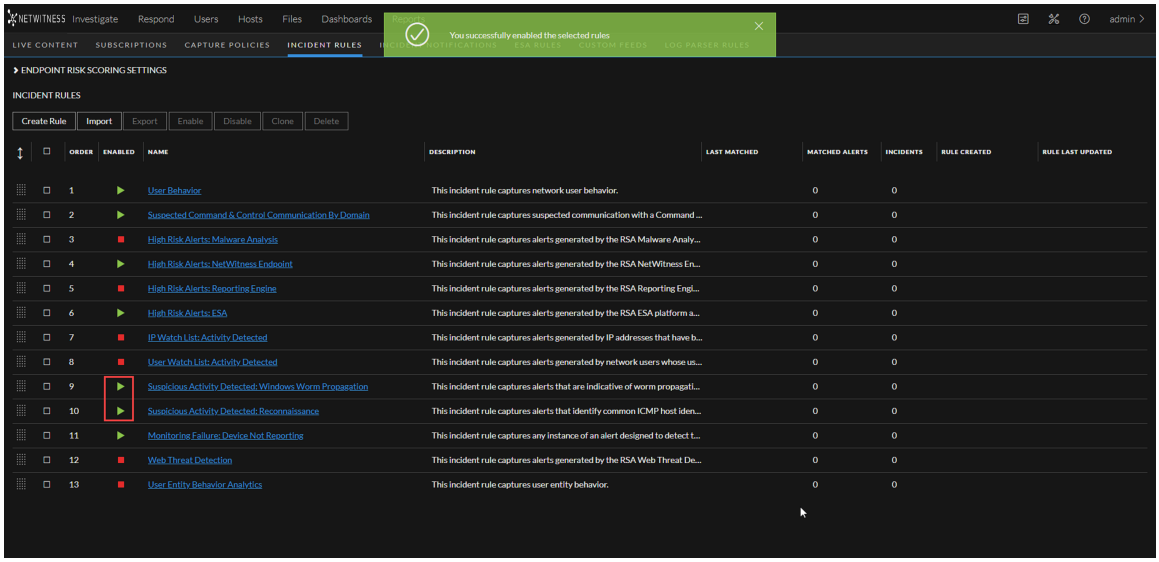
2. Select one or more incident rules and click **Enable**.



3. Click **OK** to verify that you want to enable the selected rules.



In the Incident Rules view, the Enabled column changes from a red square ■ (Disabled) to a green triangle ▶ (Enabled).



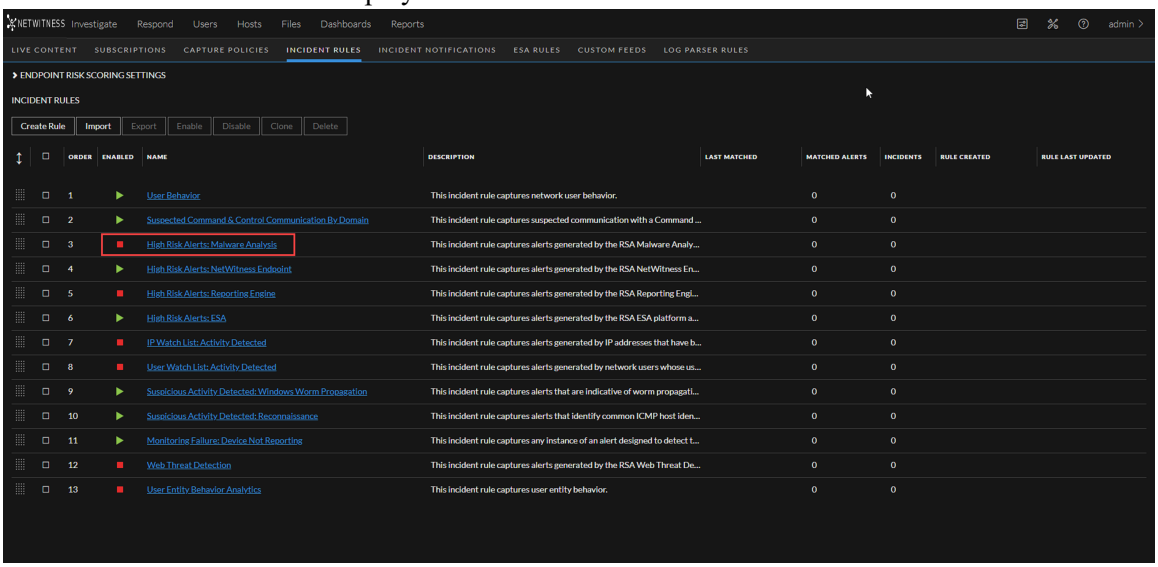
4. Verify the order of your incident rules.

Note: To disable incident rules, follow the above procedure but select the Disable button instead of the Enable button.

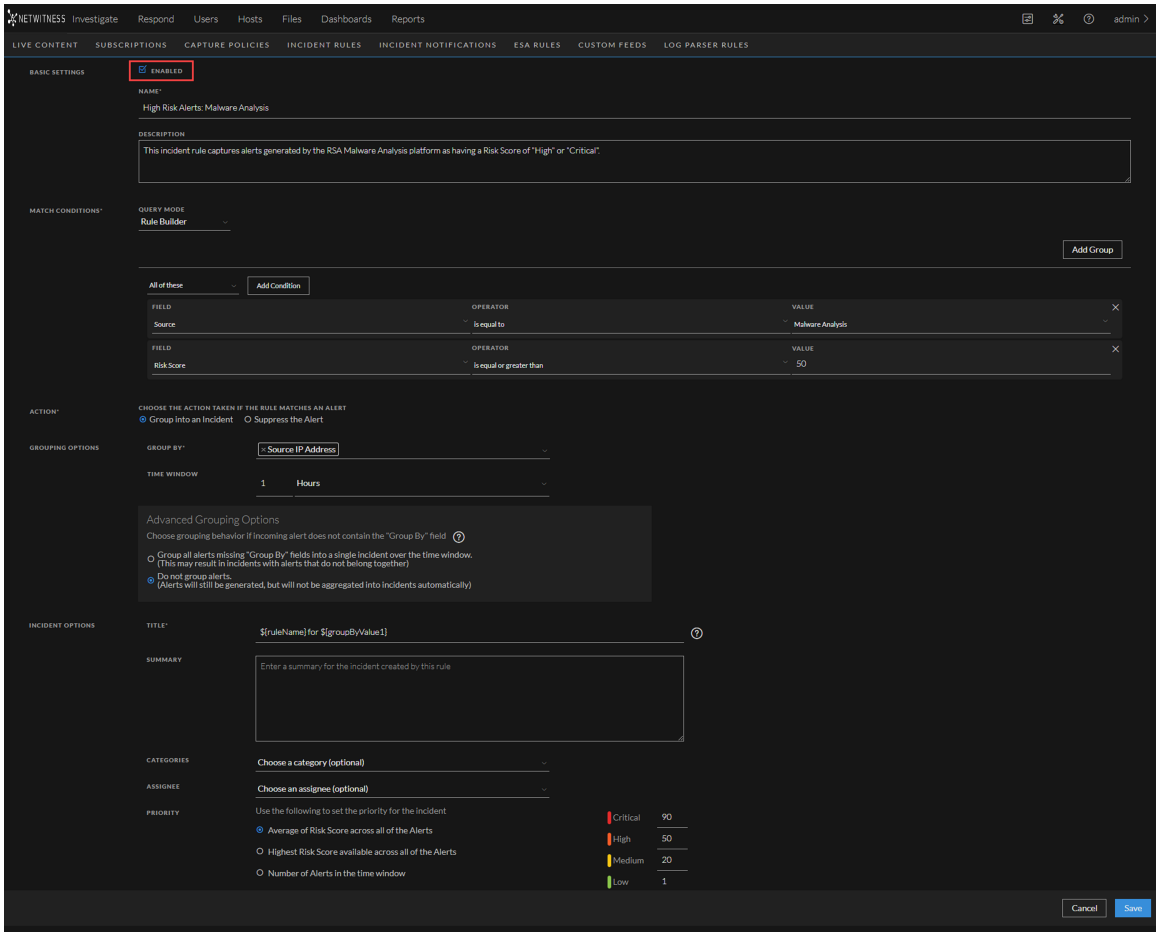
To enable an incident rule from within the incident rule details:

You can enable rules from within the incident rule details when you save your rule adjustments.

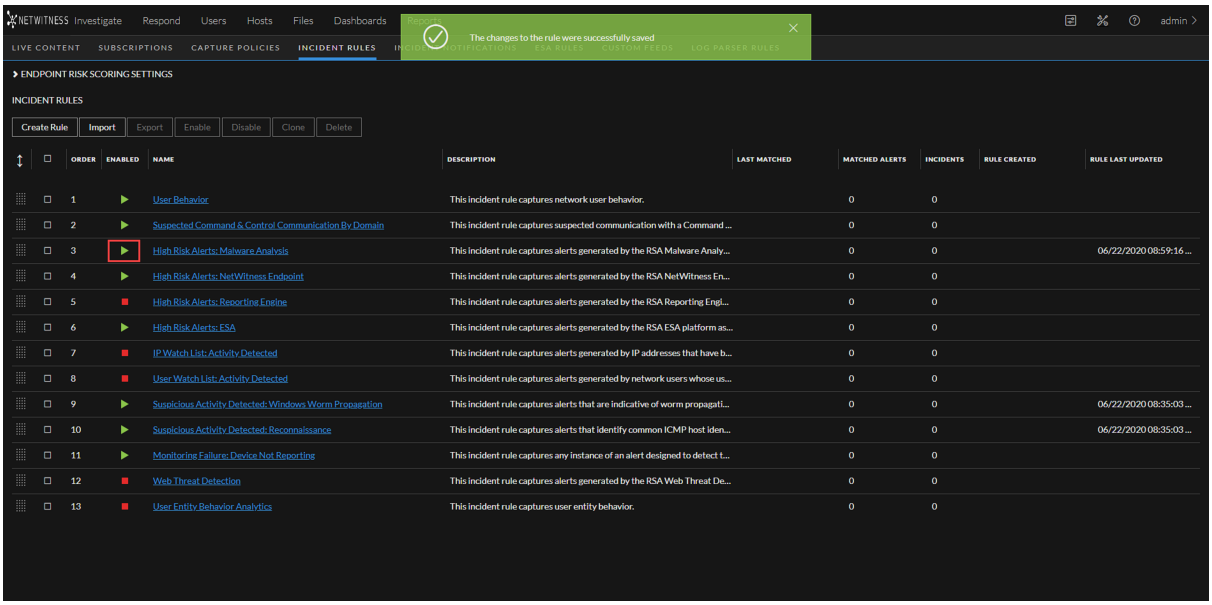
1. Go to **(Configure) > Incident Rules**.
   The Incident Rules view is displayed.



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. To adjust the default rules, see Set Up and Verify Default Incident Rules.
4. In the Basic Settings section, select the **Enabled** checkbox.
5. Click **Save** to enable the rule.
   Notice that the Enabled column changes from a red square (Disabled) to a green triangle (Enabled).



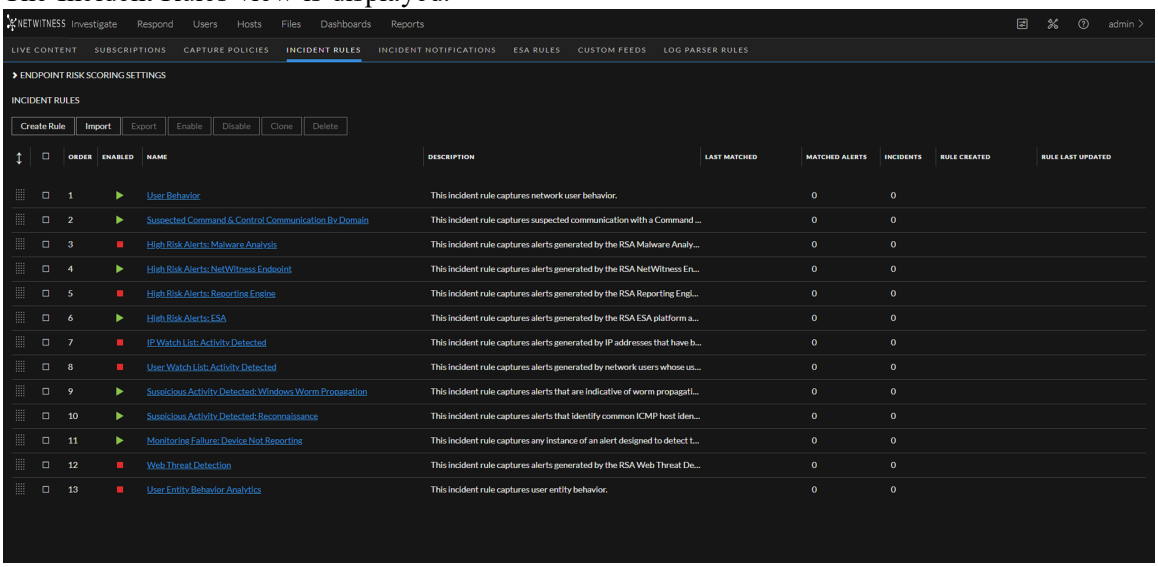
6. Verify the order of your incident rules.

Note: To disable an incident rule in the Incident Rule Details view, follow the above procedure but clear the Enabled checkbox instead of selecting it.

Create an Incident Rule

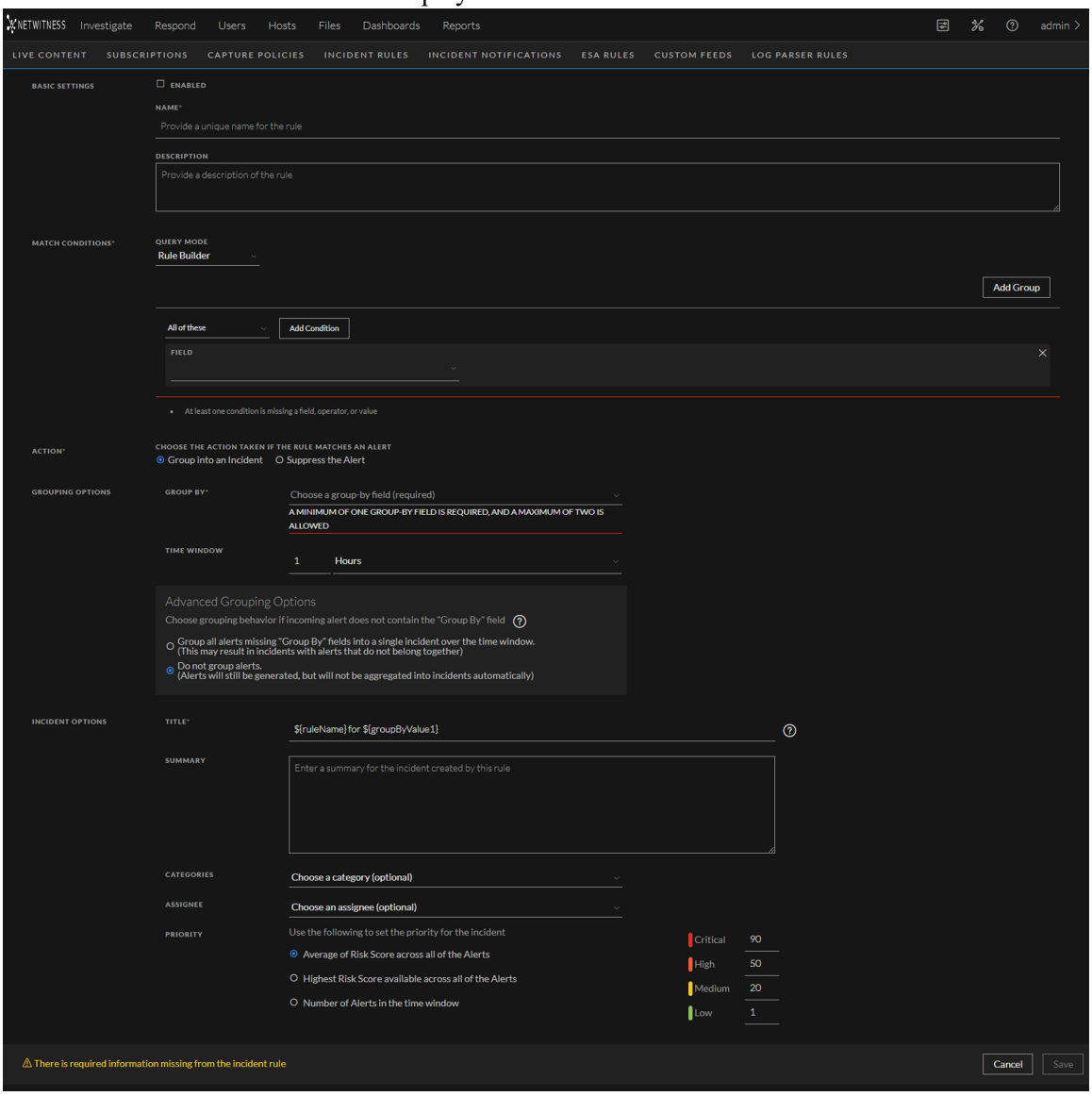
1. Go to **(Configure) > Incident Rules**.

   The Incident Rules view is displayed.



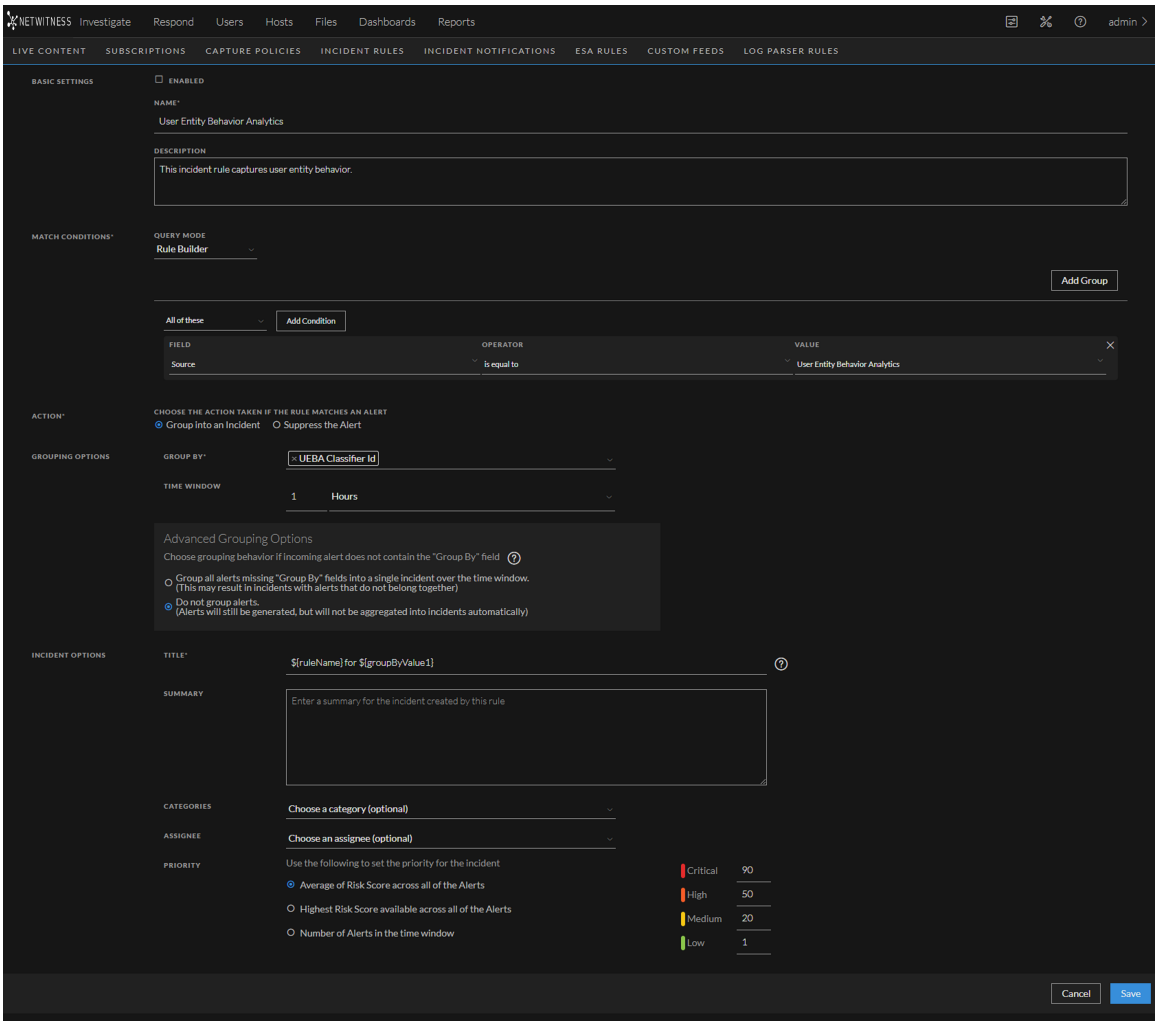
2. To add a new rule, click **Create Rule**.

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. It is the default User Entity Behavior Analytics incident rule. It captures user entity behavior grouped by Classifier ID to create incidents from alerts.



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.

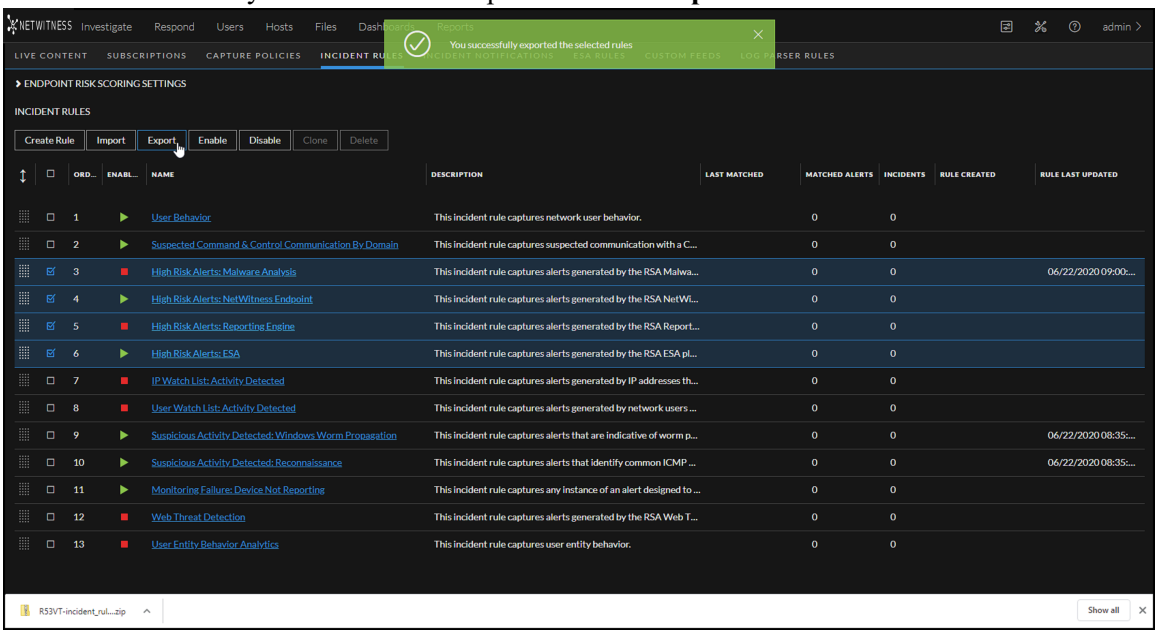
- For details on the parameter and field descriptions in the Incident Rules list, see Incident Rules View.

Export Incident Rules

Note: Exporting and importing incident rules from the Incident Rules view is only available in NetWitness version 11.4 and later.

Exporting incident rules enables you to share incident rules with other NetWitness Servers on the same release version. The exported incident rules file is a ZIP file that contains two JSON files: one file contains the incident rules and the other file contains the incident rule schema. You cannot export Advanced incident rules; the export function only allows incident rules created using Rule Builder.

1. Go to **(Configure) > Incident Rules**.
   The Incident Rules view is displayed.
2. Select the rules that you would like to export and click **Export**.



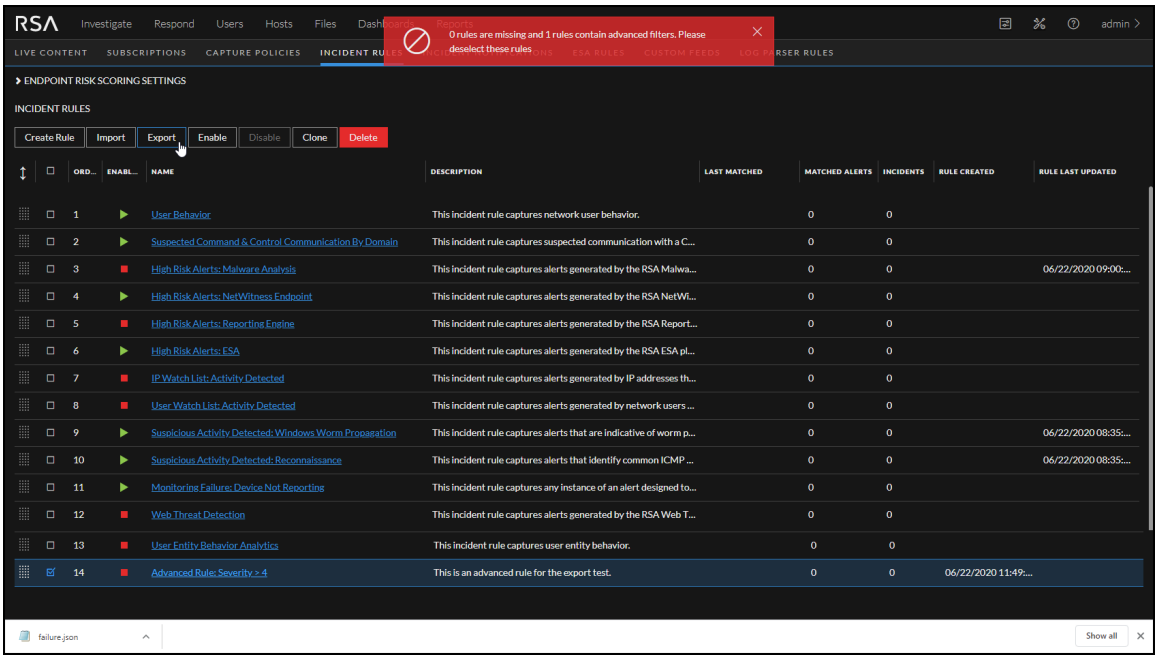
The exported incident rules file is a ZIP file in the format `<random ID>-incident_rules_export.json.zip`, which contains two mandatory JSON files:

- `aggregation_rule_schema.json` contains the incident rule schema.
- `<random ID>-incident_rules_export.json` contains the incident rules.

Note: You cannot export Advanced rules.

You can import this ZIP file on another NetWitness Server on the same release version.

If for some reason the export is not successful, and you receive only a .JSON file, for example, `failure.json`, refresh your browser and try again. This could happen if someone made an adjustment to the incident rules at the same time. You can also receive an error if you attempt to export an Advanced incident rule, which is not allowed.



Import Incident Rules

Note: Exporting and importing incident rules from the Incident Rules view is only available in NetWitness version 11.4 and later.

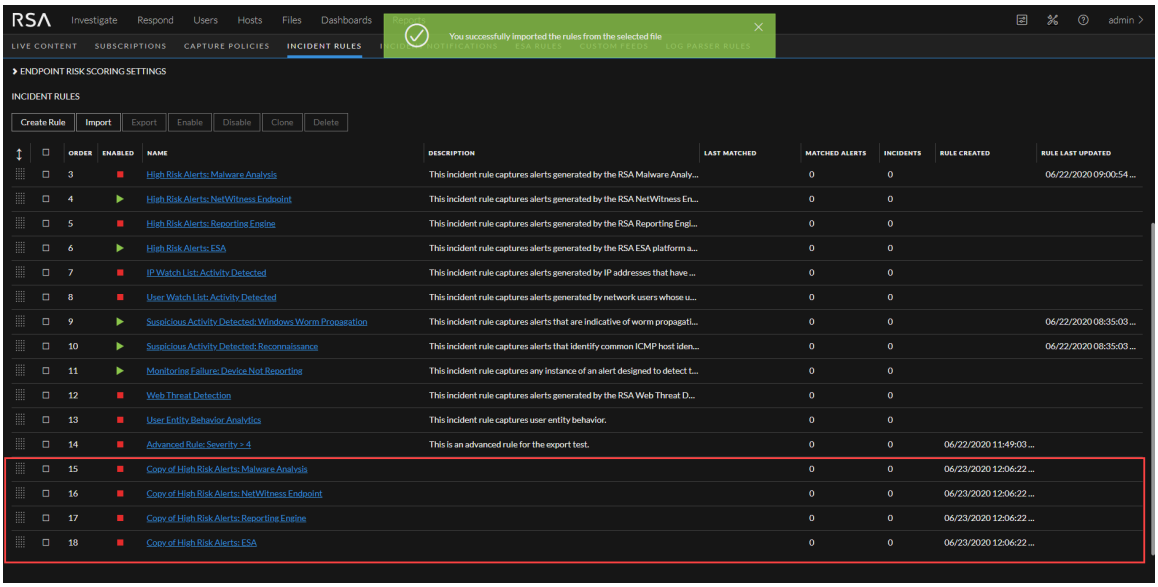
You can import an incident rules ZIP file from NetWitness Servers on the same release version. The incident rules ZIP file must be in the original exported format `<random ID>-incident_rules_export.json.zip` and contain two mandatory JSON files:

- `aggregation_rule_schema.json` contains the incident rule schema.
- `<random ID>-incident_rules_export.json` contains the incident rules.

The import fails if the ZIP file contains additional files or folders. To edit the incident rules ZIP file, see Edit the Incident Rules Export ZIP File.

To import incident rules:

1. Go to **(Configure) > Incident Rules**.
   The Incident Rules view is displayed.
2. Click **Import** and select the incident rules ZIP file to import.
   If the import is successful, a successful import notification is displayed, and the imported incident rules are disabled and shown at the bottom of the incident rules list. The **Rule Created** column shows the date and time of the import.



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 Analyst UI for Respond Server Alert Normalization
- Configure Incident 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 Archer
- Configure Threat Aware Authentication
- Set a Counter for Matched Alerts and Incidents
- Configure a Database for the Respond Server Service

Set Up and Verify Default Incident Rules

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

The Detect AI default incident rule is available in NetWitness 11.6 and later. It captures the anomalies generated by Detect AI.

The User Behavior incident rule, which captures network user behavior, is available in NetWitness 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 later 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 11.5 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**.

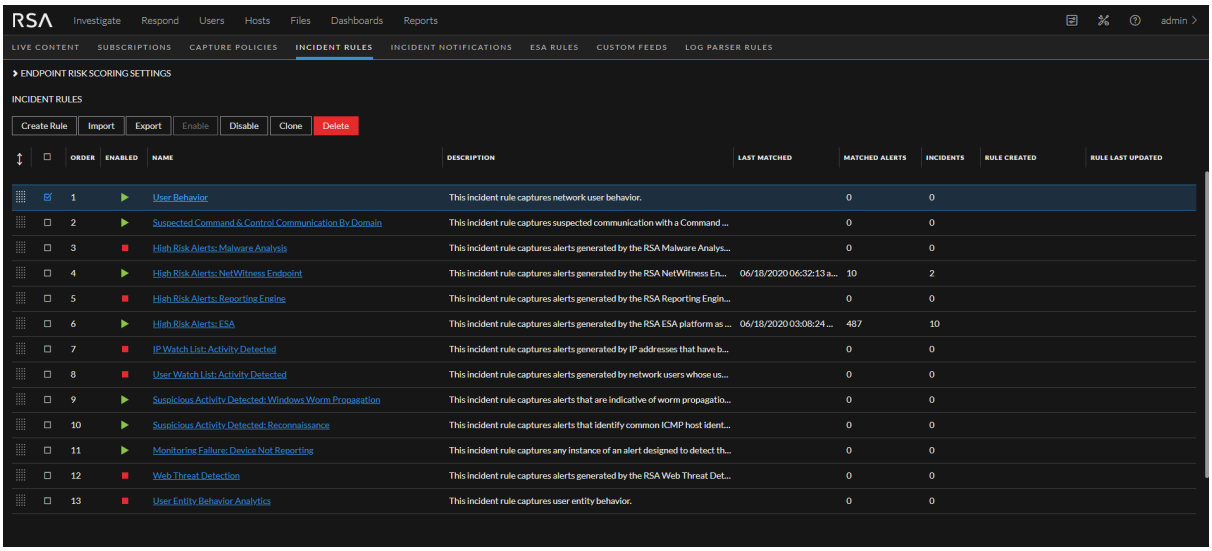
3. In the **Matching Resources** list, select the ESA Rules from the following **User Behavior** table that you are interested in monitoring and deploy them (click **Deploy**).
4. Go to **(Configure) > ESA Rules > Rules** tab, and in the Rule Library **Filter** drop-down list, select **RSA Live ESA Rule**.
5. To add a new ESA rule 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 Data Sources section, click + and add a data source to use for the ESA rule deployment.
   c. 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.

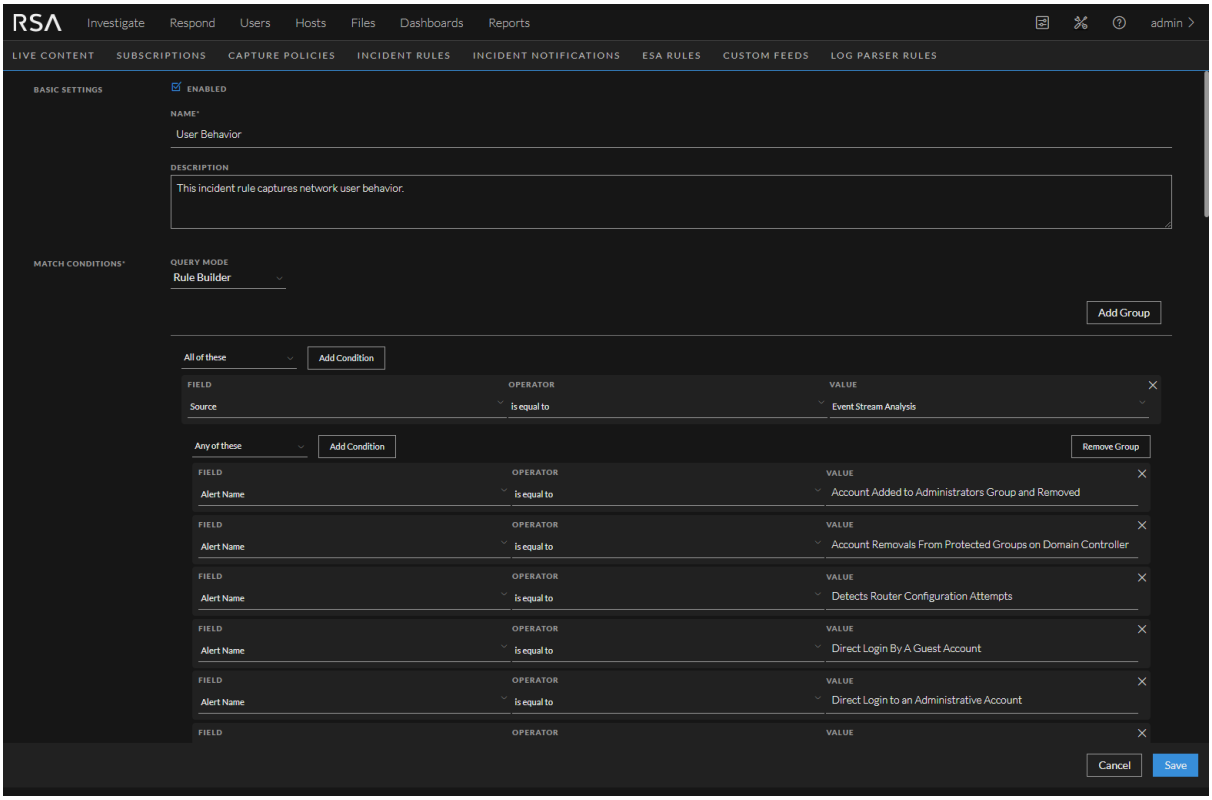
(Optional) To create the User Behavior default rule:

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.)



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. The conditions as well as the 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.

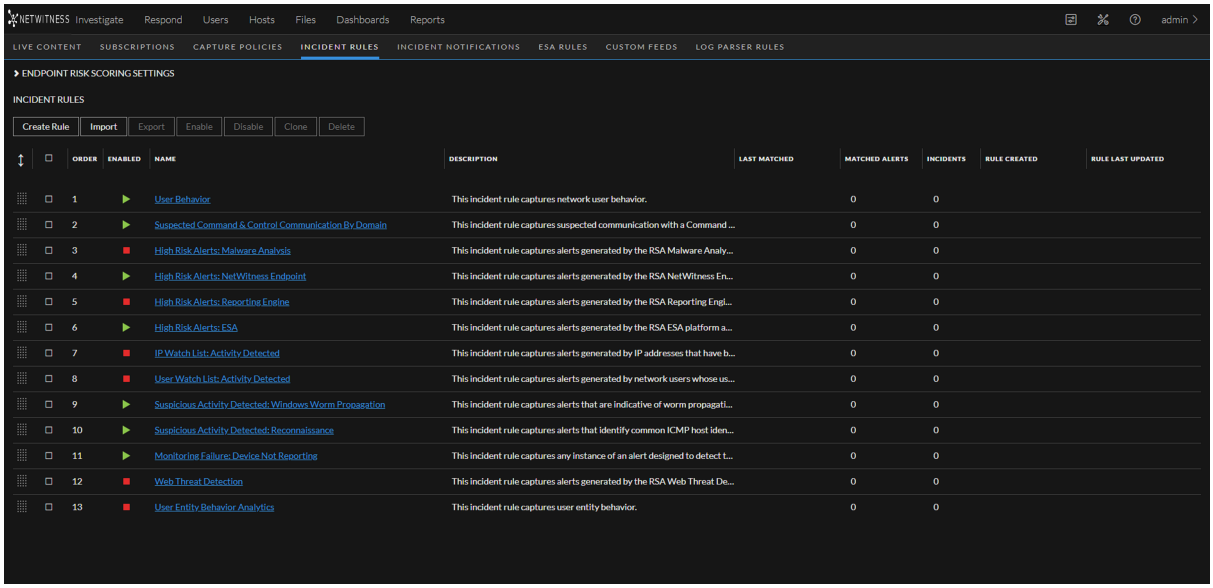
The following table shows the values for the User Behavior default incident rule.

Field	Condition Field	Condition Operator	Value
Name			User Behavior
Description			This incident rule captures network user behavior.
Query Mode:			Rule Builder **Note:** For information about advanced query mode, see Incident Rule Details View
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

Field	Condition Field	Condition Operator	Value
	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
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.



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			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 NetWitness 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 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*

Field	Condition Field	Condition Operator	Value
Time Window			1 Hour
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 NetWitness 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 NetWitness ESA platform as having a Risk Score of "High" or "Critical".
Group:			All of these

Field	Condition Field	Condition Operator	Value
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
	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

Field	Condition Field	Condition Operator	Value
	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
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 NetWitness 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
Condition:	Source	is equal to	User Entity Behavior Analytics
Group By			UEBA Classifier Id
Time Window			1 Hour
Title			${ruleName} for ${groupByValue1}

Detect AI

The following table shows the values for the Detect AI default incident rule.

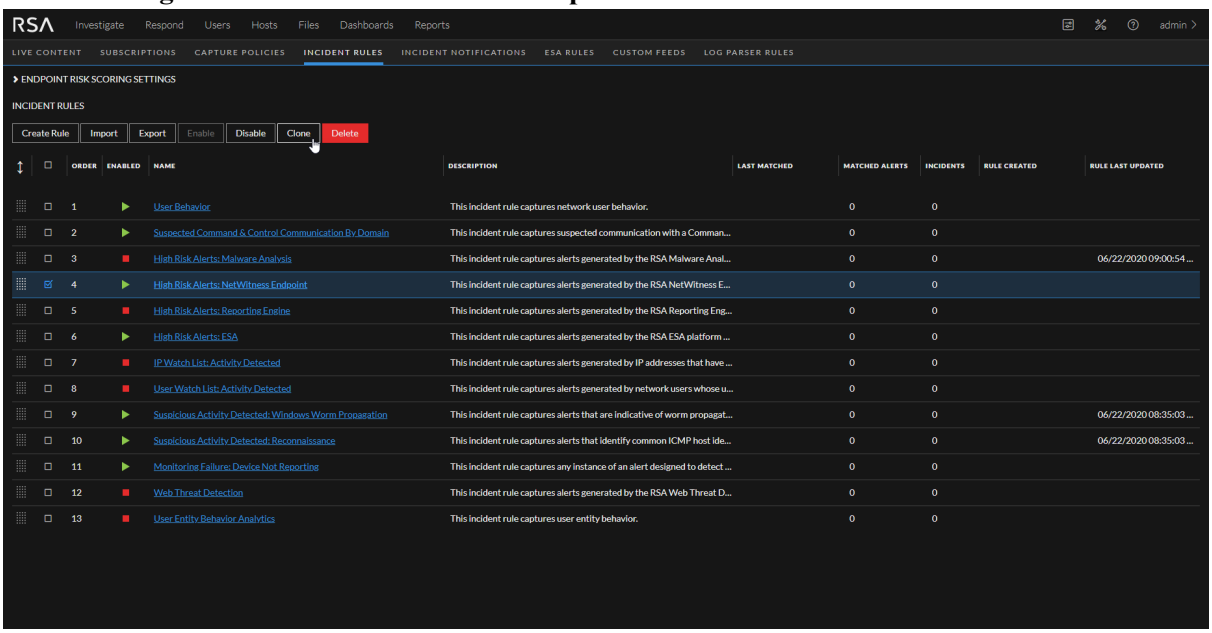
Field	Condition Field	Condition Operator	Value
Name			DetectAI
Description			This incident rule captures anomalies generated by Detect AI
Group:			All of these
Condition:	Source	is equal to	DetectAI
Group By			UEBA Classifier Id, UEBA Entity Name
Time Window			1 Hour
Title			${ruleName} for ${groupByValue2}

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, 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.

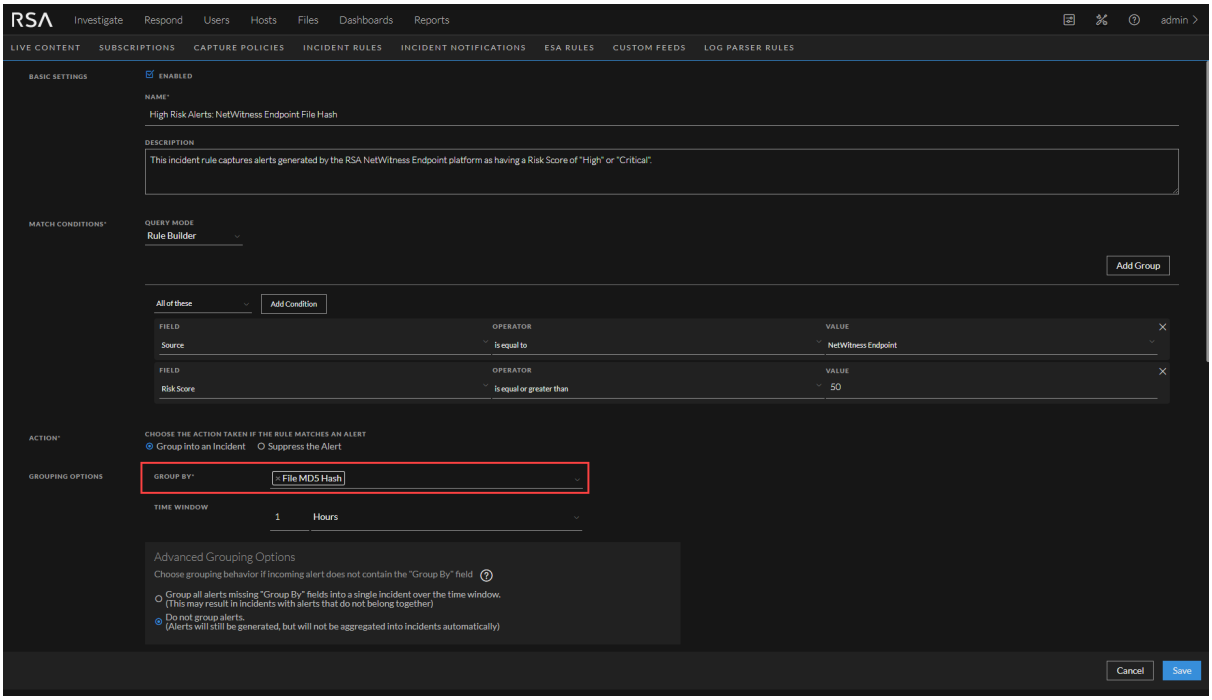
2. Select the **High Risk Alerts: NetWitness Endpoint** default incident rule and click **Clone**.



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

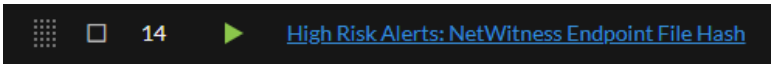
3. Change the **Name** of the rule to an appropriate name, such as High Risk Alerts: NetWitness Endpoint File Hash.

4. 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.



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 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 Risk Scoring Settings for Automated Incident Creation

Note: The information in this topic applies to NetWitness 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:

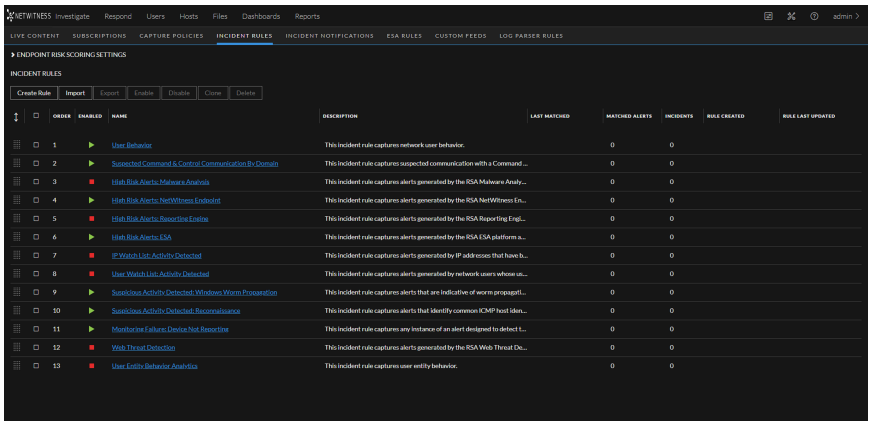
- Creates a risk scoring alert and uses it to create a risk scoring incident
- Adds risk scoring alerts along with associated events to the same incident

For more information on configuring NetWitness Endpoint, see the *NetWitnesss Endpoint Configuration Guide*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

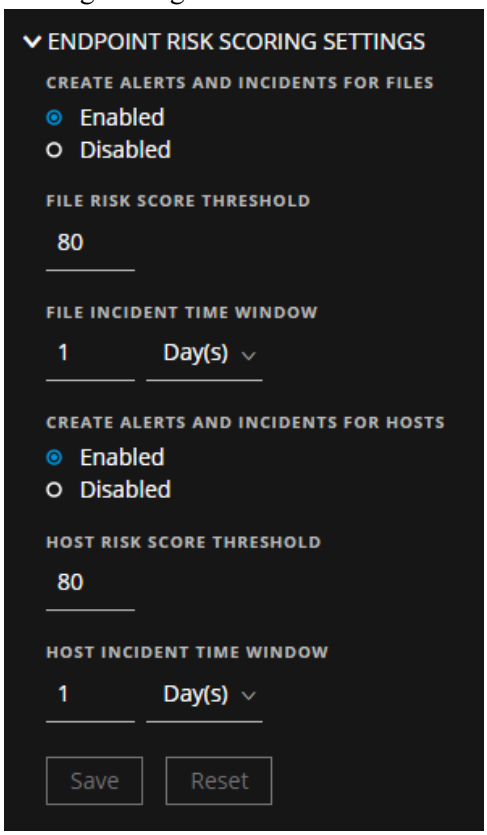
To configure the Endpoint Risk Scoring Settings:

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.



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



3. In the Endpoint Risk Scoring Settings section, adjust the settings as follows:

   a. **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.

b. **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.

c. **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 Custom Respond Server Alert Normalization

Note: This procedure is optional. Administrators can use it to change Respond Server alert normalization.

Analysts who are content experts can create ESA Correlation rules that generate alerts. When a rule is more complex than what can be specified in the ESA Rule Builder, they can write advanced Event Process Language (EPL) rules. After the ESA rules are deployed and the alert criteria is met, ESA Correlation-server forwards the raw alerts to Respond-server.

The schema, meta key selection, and event pattern of the raw alerts are unknown to the Respond-server since they depend on the way the ESA rules are written. In this case, you can customize the logic to parse the raw alert to an acceptable format. The parsing (normalization) logic is written in JavaScript language and NetWitness users who know how to write JavaScript code can customize the Respond normalization script files.

In NetWitness version 11.4 and later, to prevent overwriting future customizations in the Respond normalization scripts, add any custom logic to the **`custom_normalize_<alert type>.js`** files. The custom normalization script files have a `custom_normalize` prefix and are located in the **`/var/lib/netwitness/respond-server/scripts`** directory:

```
data_privacy_map.js
custom_normalize_alerts.js
custom_normalize_core_alerts.js
custom_normalize_ecat_alerts.js
custom_normalize_ma_alerts.js
custom_normalize_ueba_alerts.js
custom_normalize_wtd_alerts.js
utils.js
```

For Example, the `custom_normalize_core_alerts.js` is the normalization script used to add custom logic for ESA alerts. This JavaScript file has a `normalizeAlert` function with the parameters `headers`, `rawAlert`, and `normalizedAlert`. The `normalized` variable is an immutable copy object which has an embedded object with a list of normalized events. So if you have any custom meta keys configured for the events then you have to iterate through the `normalized.events` to populate the appropriate meta keys with values from the `rawAlert.events` object. The following figure shows sample code.

Sample Custom Normalize Core Alerts Code

```
normalizeAlert = function (headers, rawAlert, normalizedAlert) { // normalizedAlert is the immutable copy of ootb normalizer alert, make sure you use // normalized object to update/set the values in your scripts var normalized = Object.assign(normalizedAlert); var custom_events; if(normalized.events !== undefined) { custom_events = normalized.events; } else { custom_events = new Array([]); } for (var i = 0; i < rawAlert.events.length; i++) { custom_events[i].legalentity=Utils.stringValue (rawAlert.events[i].isgs_legalentity); custom_events[i].companycode=Utils.stringValue (rawAlert.events[i].isgs_companycode); } if(normalized.events === undefined){ normalized.events = custom_events; } return normalized; };
```

To Configure Custom Respond Server Alert Normalization:

1. Open the `custom_normalize_core_alerts.js` file.

custom_normalize_core_alerts.js

```
exports.normalizeAlert = function (headers, rawAlert, normalizedAlert) { //
normalizedAlert is the immutable copy of ootb normalizer alert, make sure you use //
normalized object to update/set the values in your scripts var normalized = Object.assign
(normalizedAlert); // Add custom logic below return normalized; };
```

The `normalizedAlert` object has been broadcasted, which already comes through the basic parsing logic flow where some of the meta values have been copied to `normalizedAlert` from `headers` and `rawAlert`.

2. Populate The `normalizedAlert` object with the custom meta values that are not covered in the basic parsing logic:
   a. Add your custom logic below the line: `var normalized = Object.assign (normalizedAlert);`

      The `headers` parameter has very few attributes like:

      `headers.severity`

      `headers.deviceProduct`

      The important parameter is `rawAlert`, which has an embedded `events` object, which is an array. It is basically the list of events associated with the alert. The `events` object has all meta keys governed from the Concentrator. Here are some example meta keys:

      `event.user_dst`
      `event.user_src`
      `event.username`
      `event.domain_dst`
      `event.domain_src`
      `event.host_dst`
      `event.host_src`
      `event.analysis_session`
      `event.analysis_service`
      `event.analysis_file`
      `event.agent_id`
      `event.device_type`
      `event.category`
      `event.action`
      `event.user`
      `event.owner`
      `event.port_dst`
      `event.OS`

`event.process_vid_src`

To view the look-up table for meta keys, go to  **(Configure) > Esa Rules > Settings > Meta Key References**.

The `normalized` object also has an embedded `events` object, which is an array.

b. Iterate through each item of the `normalized.events` and `rawAlert.events` and then copy the custom meta attributes from the `rawAlert.events` to the `normalized.events`.

The following example shows how to add custom meta keys to the `custom_normalize_core_alerts.js` file.

Example of Custom Alert Normalization

```
exports.normalizeAlert = function (headers, rawAlert, normalizedAlert) { // normalizedAlert is the immutable copy of ootb normalizer alert, make sure you use // normalized object to update/set the values in your scripts var normalized = Object.assign (normalizedAlert); var custom_events; if (normalized.events != undefined) { custom_events = normalized.events; } else { custom_events = new Array(); } // iterate through each item for (var i = 0; i < rawAlert.events.length; i++) { custom_events [i].metaKey1=Utils.stringValue(rawAlert.events[i].rawCustomMetaKey1); // Utils is a helper module to stringify the object custom_events[i].metaKey2=Utils.stringValue (rawAlert.events[i].rawCustomMetaKey2); } If (normalized.events == undefined) { normalized.events = custom_events; } return normalized; };
```

The `metaKey1` and `metaKey2` meta keys are now assigned meta keys, which you can view in the NetWitness user interface.

When customizing normalization script files, you can also look at the built-in Respond normalization script files for reference, such as `normalize_alerts.js`.

Configure Analyst UI for Respond Server Alert Normalization

This procedure is optional. Administrators can use it to change Respond Server alert normalization on the Analyst UI.

Note: This option is available in NetWitness version 11.4 and later.

The Analyst UI (Analyst User Interface) enhances the performance of investigations for analysts who work in locations geographically separated from the NetWitness Server host. Respond Server alert normalization is disabled by default on the Analyst UI, but with enough bandwidth you can configure the Respond Server on the Analyst UI to normalize alerts for potential performance gains.

Respond Server alert normalization at the Analyst UI should be very carefully considered. If the Analyst UI is deployed in an environment that is geographically separated from the NetWitness Server (NW Server) and ESA services, depending on available bandwidth, normalizing alerts at the Analyst UI can generate large volumes of traffic, potentially impacting other services on the network. Potential gains from normalizing alerts at the Analyst UI can result in a performance decrease on the NW Server and ESA services.

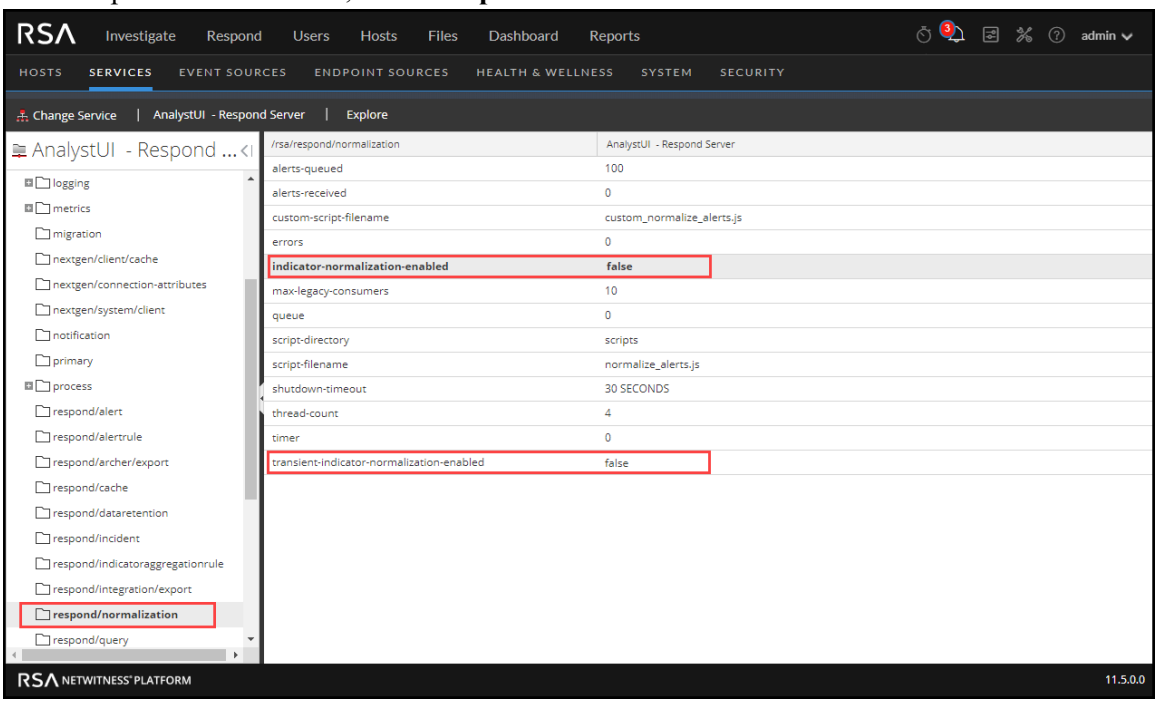
You can configure whether to normalize alerts for any Respond Server (NW Server or Analyst UI) by enabling or disabling alert normalization.

- Normalization is enabled by default for the Respond Server running on the NW Server host.
- Normalization is disabled by default for the Respond Server running on the Analyst UI.

To change the alert normalization settings for the Respond Server running on the Analyst UI:

1. Log in to NetWitness on the NW Server host as administrator.
2. Go to  **(Admin) > Services**, select the Respond Server service running on the Analyst UI, and then select  **> View > Explore**.

3. In the Explore view node list, select **respond/normalization**.



   a. To turn on alert normalization for ESA and other alert generating sources, in the **indicator-normalization-enabled** field, enter **true**. To turn it off, enter **false**.

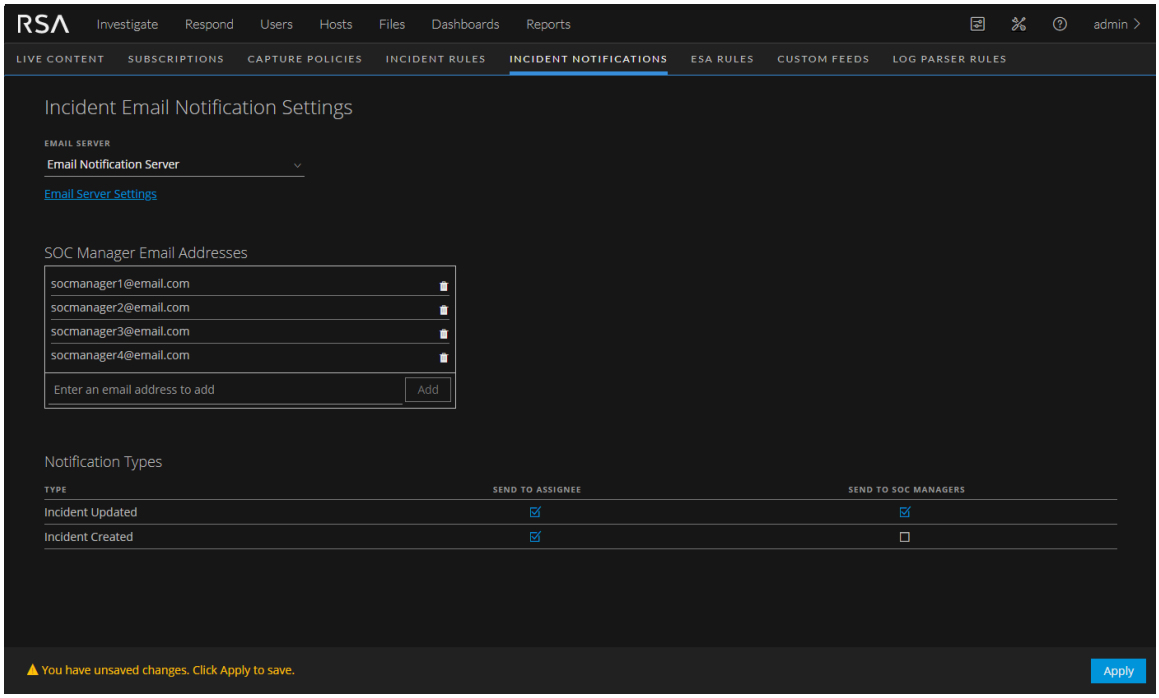
   b. To turn on alert normalization coming from event correlation for risk scoring alerts, in the **transient-indicator-normalization-enabled** field, enter **true**. To turn it off, enter **false**.

4. Restart the Respond Server service on the Analyst UI for the new settings to take effect. To do this, go to  **(Admin) > Services**, select the Respond Server service on the Analyst UI, and then select  **> Restart**.

Configure Incident Email Notification Settings

Incident email 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) > Incident Notifications**.
   The Incident Email Notification 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 and go to the **Servers** tab. For more information, click the help icon or refer to the *System Configuration Guide*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.
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 version 10.6.x to 11.1 and later. The Incident Management Notification Settings in 10.6.x are different from the Incident Email Notification settings available in 11.1 and later. You will need to manually update the incident 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.

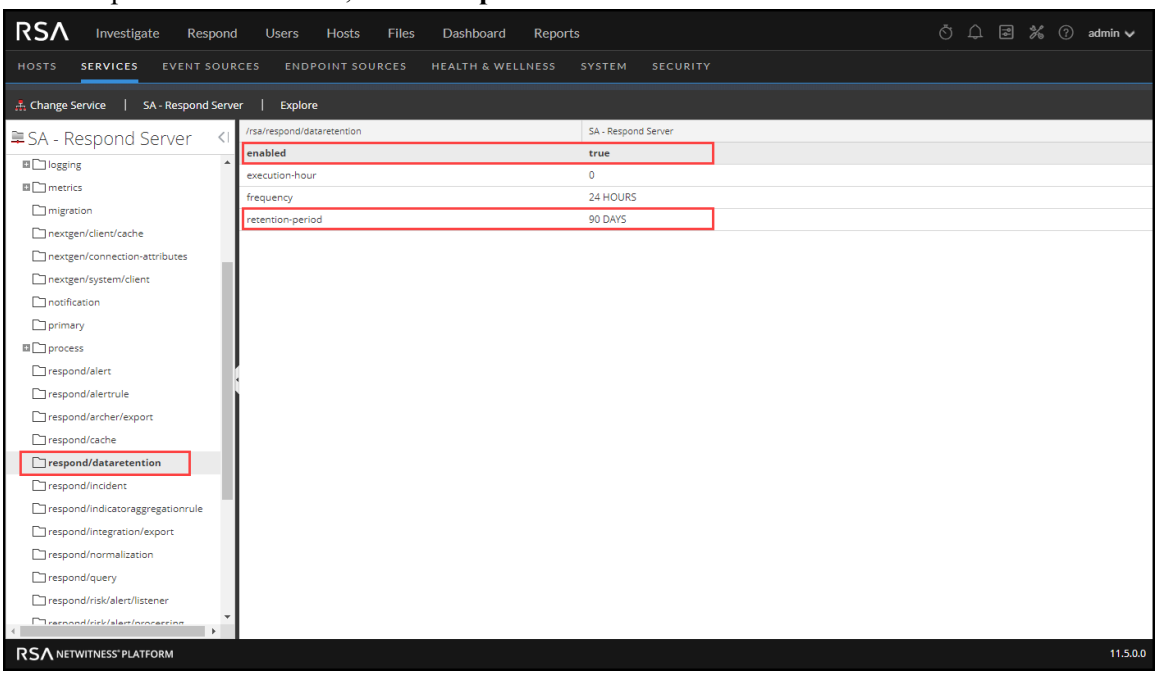
Prerequisites

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.
   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.

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 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. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

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.

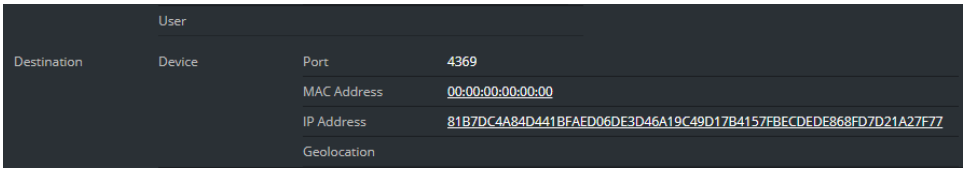
Prerequisites

- 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 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. In NetWitness 11.4 and later, you can manually create incidents from Respond and Investigate.

For more detailed integration information, see the *NetWitness Archer Integration Guide*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Prerequisites

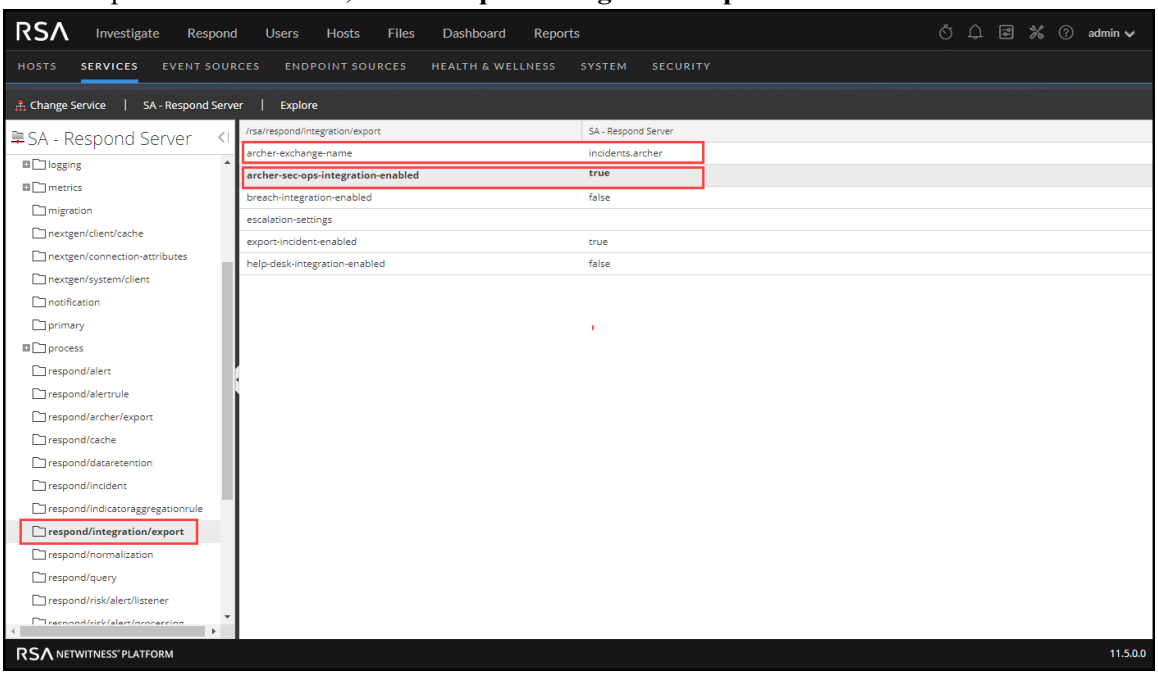
- Archer Cyber Incident & Breach Response 1.3.1.2 (NetWitness 11.0 works only with Archer Cyber Incident & Breach Response 1.3.1.2.)

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 Archer

Note: The information in this topic applies to NetWitness Version 11.2 and later.

If you want to manage incidents in NetWitness Respond, you have the option to configure the NetWitness so that you can send incidents to Archer Cyber Incident & Breach Response. If 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*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Prerequisites

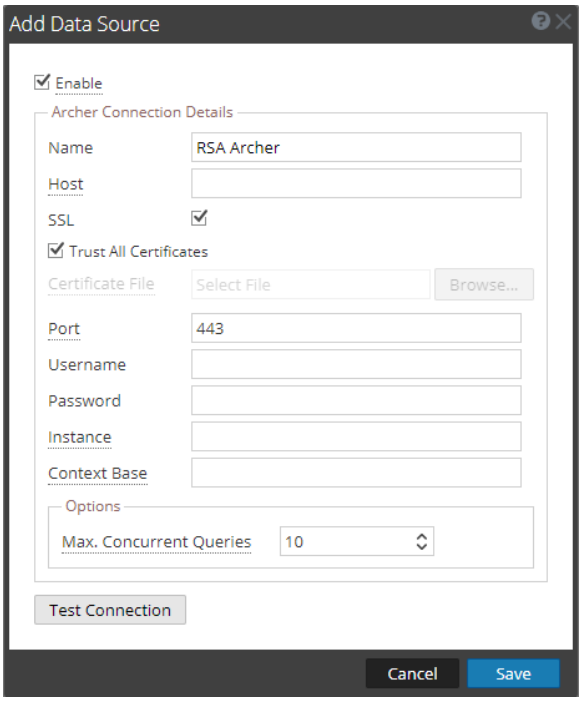
- Archer release 6.6 P4, 6.6 P5, or 6.7 P2 only is required for NetWitness 11.4 and 11.5.
- Archer release 6.4 or later is required for NetWitness 11.2 and 11.3.

Add Archer as a Data Source for Context Hub

To configure sending incidents to Archer Cyber Incident & Breach Response from NetWitness Respond, Archer must be configured as a data source for Context Hub. For more detailed instructions for configuring the Archer data source, see the "Configure Archer as Data Source" topic in the *Context Hub Configuration Guide*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

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 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 Archer

content for a specific instance.

- **Context Base**: Enter the virtual directory name where the files are stored. For example, rsaarcher located at the 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**.
   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 NetWitness 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 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`

```
[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 ~]#
```

3. Enter `rsa.security.pki.use-jvm-trust: true` to enable the configuration.
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.securid.com/t5/securid-cloud-authentication/manage-the-cloud-administration-api-keys/ta-p/623066 and "Determining Access Requirements for High-Risk Users in the Cloud Authentication Service" topic at https://community.securid.com/t5/securid-cloud-authentication/determining-access-requirements-for-high-risk-users-in-the-cloud/ta-p/623067.

Configure RSA SecurID Access API Key

To configure RSA SecurID Access API key using NetWitness Shell:

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

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`.
4. Type `login` and enter admin username and password.
5. 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.

6. 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.
7. 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 NetWitness Community.

Configure Sync Frequency

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

To edit the frequency:

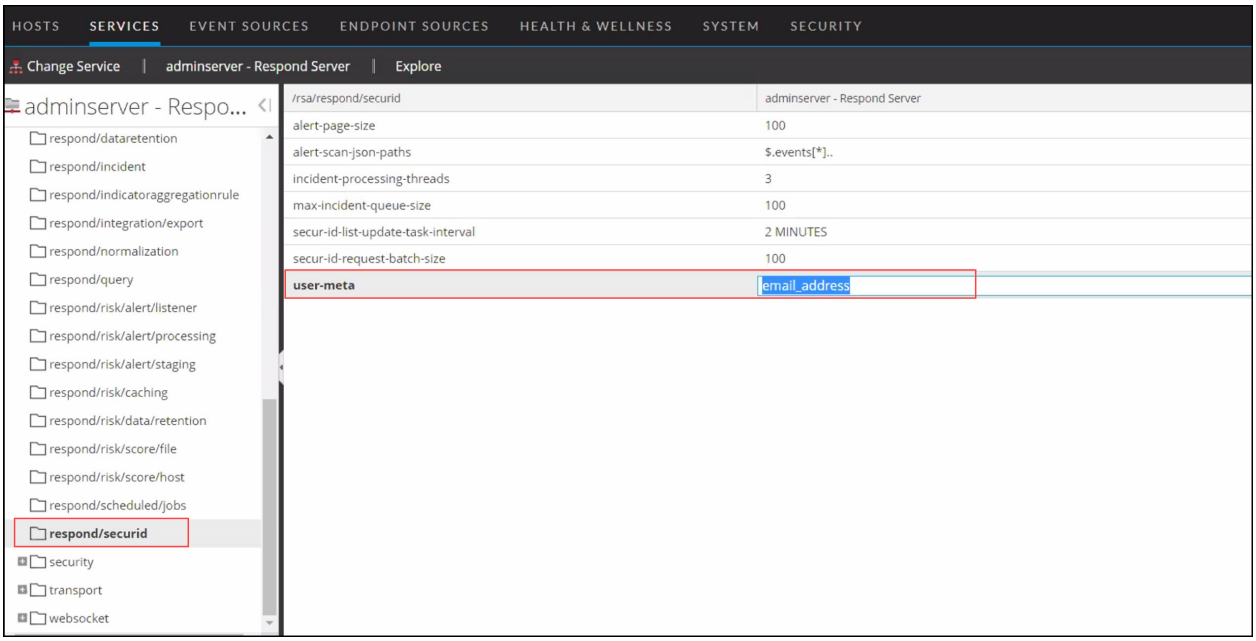
1. Log in to NetWitness.
2. Go to  (Admin) **> Services**, select the Respond Server service, and then select >  **> View > Explore**.
3. Edit the duration at **rsa/respond/securid**.

Configure Meta

You can configure a respond specific meta in an alert to identify a user to be added to SecurID high-risk user's list. By default, the meta is set to `email_address`. Currently, the Respond Server supports metas such as ad_username, and email_address.

To add a Respond Server supported meta:

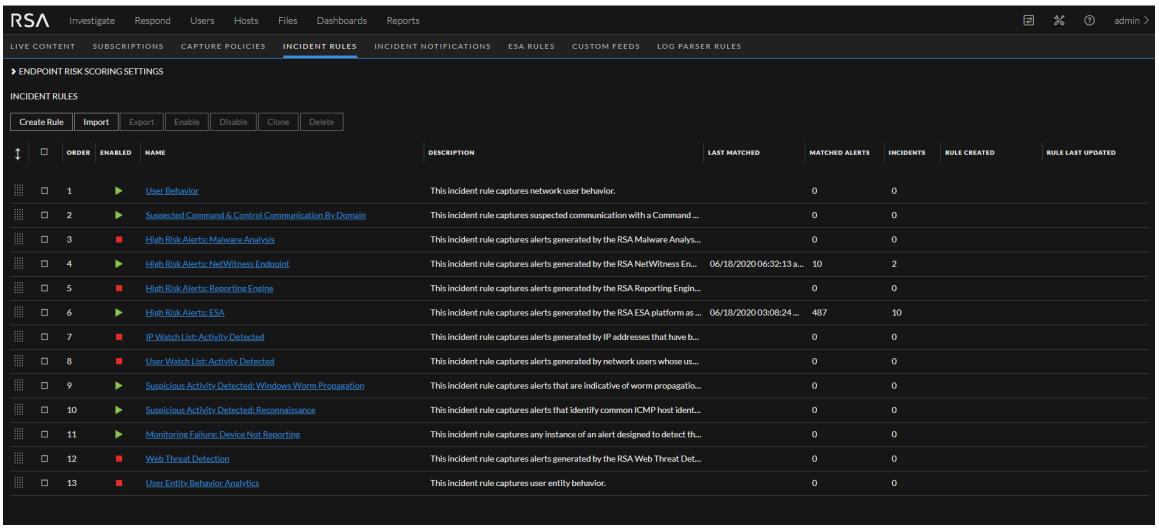
1. Log in to NetWitness Platform.
2. Go to  **(Admin) > Services**, select the Respond Server service, and then select >  **> View > Explore**.
3. In the Explore view node list, select **respond/securid**.
4. Edit and enter a meta in the **user-meta** field.



Note: If at any time you change the meta configuration from email address to ad_username, make sure to run Step 7 from Configure RSA SecurID Access API Key to process the older incidents. In case of a multi-analyst deployment, make sure you configure the same meta on all Respond servers. For example, if you update the meta to ad_username, then the same must be updated on all Respond servers.

Set a 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.



The following columns provide matched alert 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.

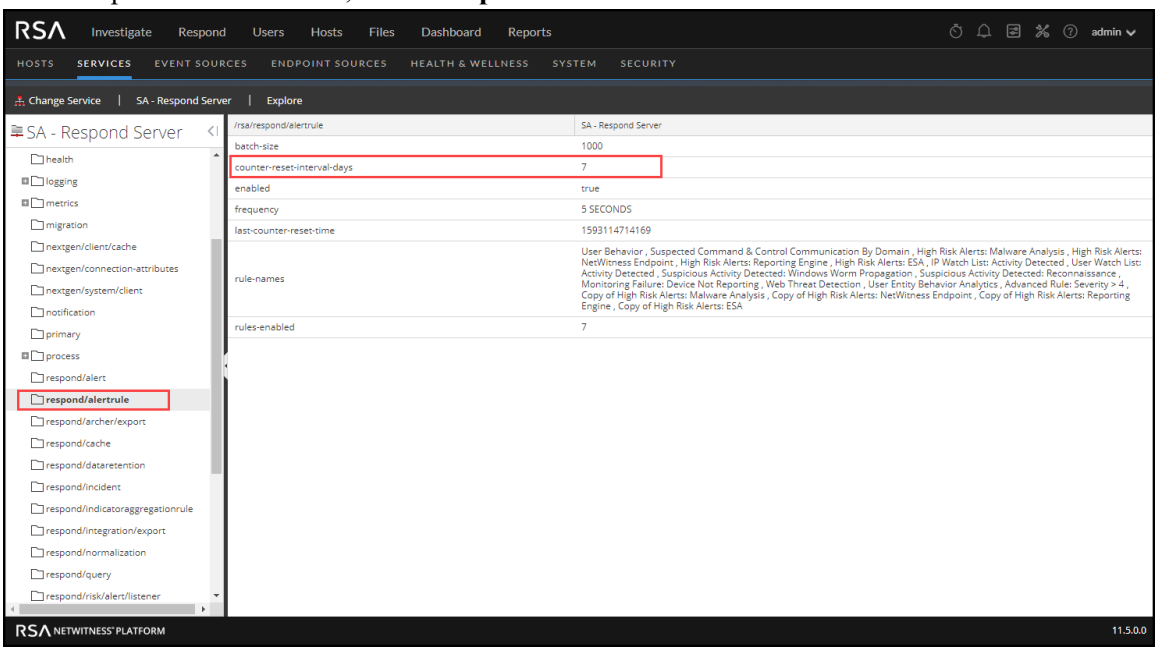
By default, these values reset to zero every 7 days. Depending on how long you want the counts to continue, you can change the default number of days.

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**.

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**.

Edit the Incident Rules Export ZIP File

This procedure is optional and is for advanced users. When exporting incident rules from the Respond Incident Rules view, the exported incident rules file is a ZIP file in the format `<random ID>-incident_rules_export.json.zip`, which contains two mandatory JSON files:

- `aggregation_rule_schema.json` contains the incident rule schema.
- `<random ID>-incident_rules_export.json` contains the incident rules.

You can import this ZIP file on another NetWitness Server on the same release version.

There may be situations when you need to edit the these files before you import them to another NetWitness Server.

To edit the incident rules export files:

1. Follow the Incident Rule Export Files Editing Guidelines below to edit the export files.
2. Before importing, verify that the ZIP file does not contain additional files or folders. The ZIP file should contain only the mandatory `aggregation_rule_schema.json` and `<random ID>-incident_rules_export.json` files to go through the import. Any files other than these two cause the import to fail.
   For example, when compressing files on a Mac, it adds a temp folder `__MACOSX` that needs to be excluded while zipping the file.

Note: You cannot export Advanced rules.

Incident Rule Export Files Editing Guidelines

Ensure that the following fields have at least one value. Removing a value or having an empty value for the following fields results in abnormal behavior.

Field	Possible Values
name	`A-Z a-z 0-9 " !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~"`
groupByFields	A Minimum of 1 or a Maximum of 2 group_by keys should be present in `aggregation_rule_schema.json`.
timeWindow	A String value in the following accepted formats: Days – Min:`1d` Max: `24d` Hours – Min: `1h` Max: `100h` Minutes – Min: `1m` Max :`100m`

action	Should be one of following values:
	`GROUP_INTO_INCIDENT`
	`SUPPRESS_ALERT`

Field	Possible Values
incidentScoringOptions	Should be one of the following string values: `average`: Average of Risk Score across all of the Alerts `high`: Highest Risk Score available across all of the Alerts `count`: Number of Alerts in the time window
priorityScale	Condition: LOW < MEDIUM < HIGH < CRITICAL

	Sub Fields — **Possible Values**
	`MEDIUM` — `1-100`
	`CRITICAL` — `1-100`
	`HIGH` — `1-100`
	`LOW` — `1-100`

uiFilterConditions	Sample UI Conditions Filter Structure

	Sub Fields — **Possible Values**
	`filterType` — `FILTER`
	`FILTER_GROUP`
	Possible values for `FILTER` are listed below.
	`property` — `value`: fetched from `aggregation_rule_schem.json`
	`operator` — `operators`
	`value` — `type`: dictates the data type.
	Available options:
	`textfield`: String
	`combobox` : from a list of options available in the json
	`datefield`: unix time stamp, for example: 2019-06-12T12:00:00Z
	`numberfield`: Integer

incidentCreationOptions	`ruleSummary`: String `categories`: JSON `array assignee`: JSON

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.

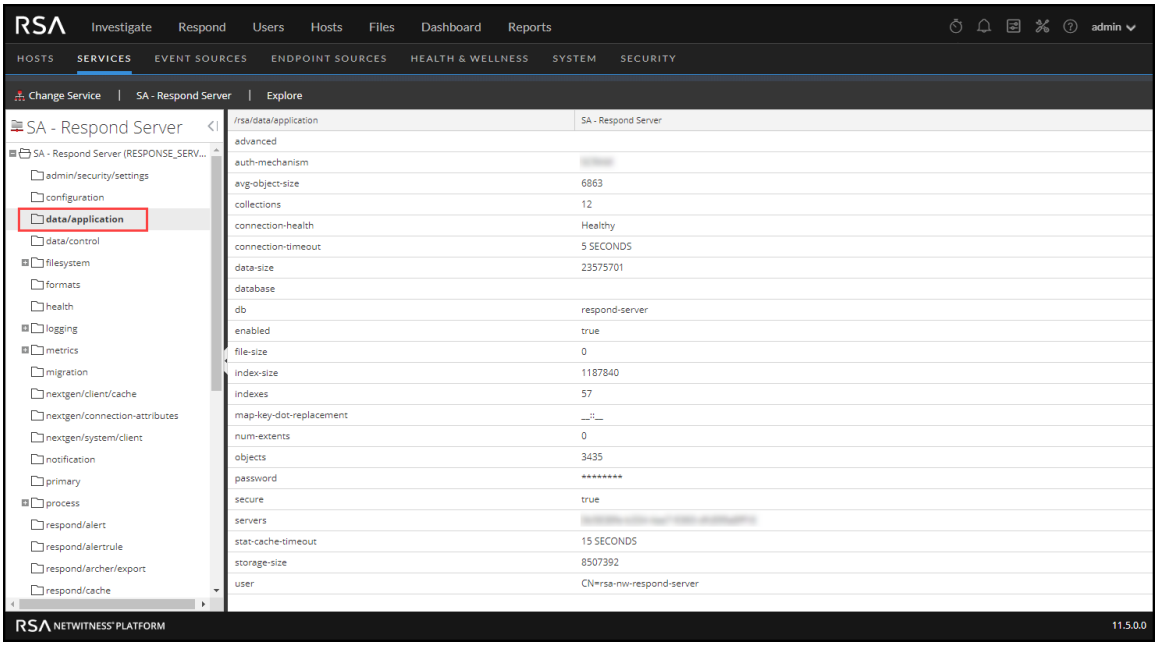
Prerequisites

Ensure that:

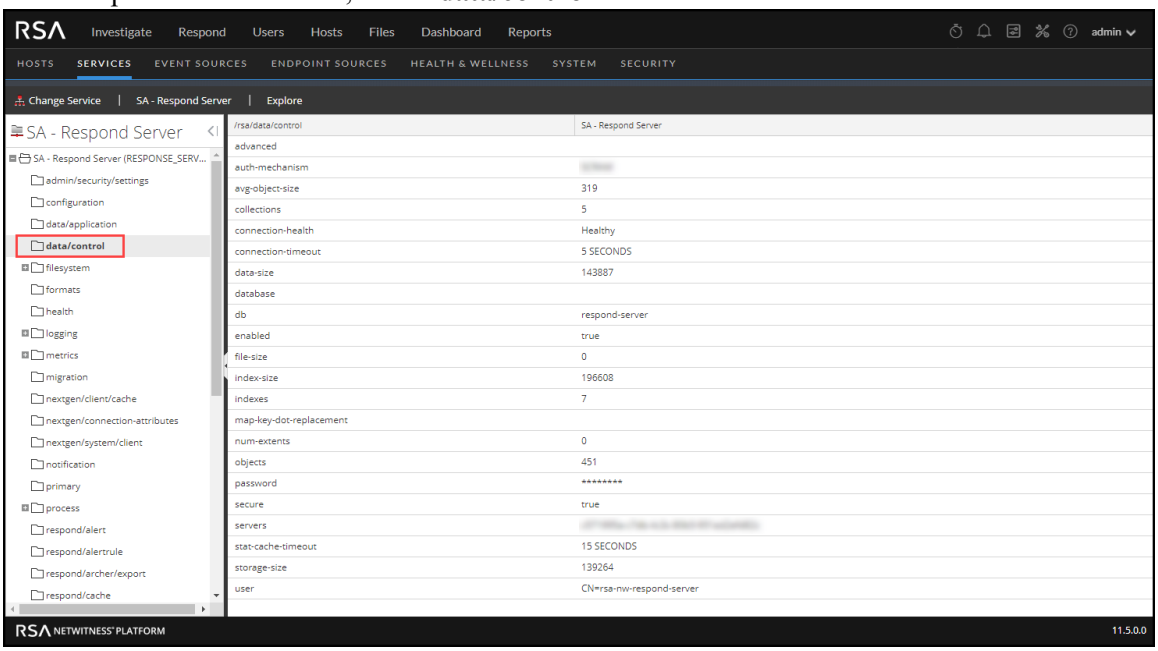
- The Respond Server service is installed and running on NetWitness.
- An ESA host is installed and configured.

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

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

- **Incident Rules**: NetWitness 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 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 NetWitness 11.1 and later.

What do you want to do?

Role	I want to ...	Show me how
Analyst, Content Expert, SOC Manager	Create, edit, enable, export, or import an incident rule.	Step 3. Enable and Create Incident Rules for Alerts
Analyst, Content Expert, SOC Manager	Configure the threshold that creates risk scoring alerts and incidents to adjust the amount of alerts and incidents created. Turn off the creation of risk scoring alerts and incidents. Endpoint Risk Scoring Settings only apply to NetWitness Endpoint.	Configure Risk Scoring Settings for Automated Incident Creation
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*.

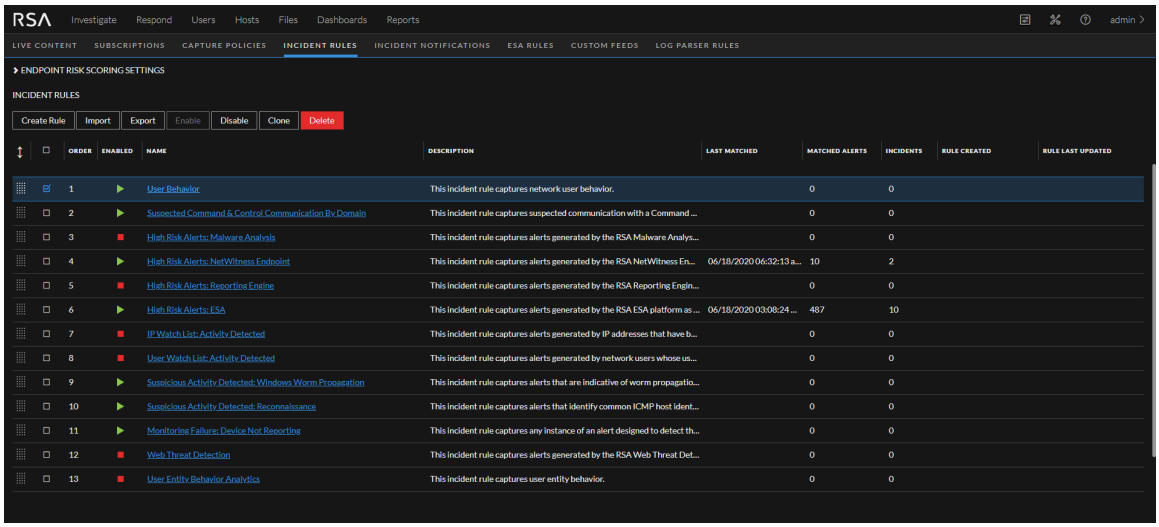
Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Related Topics

- Incident Rule Details View

Quick Look

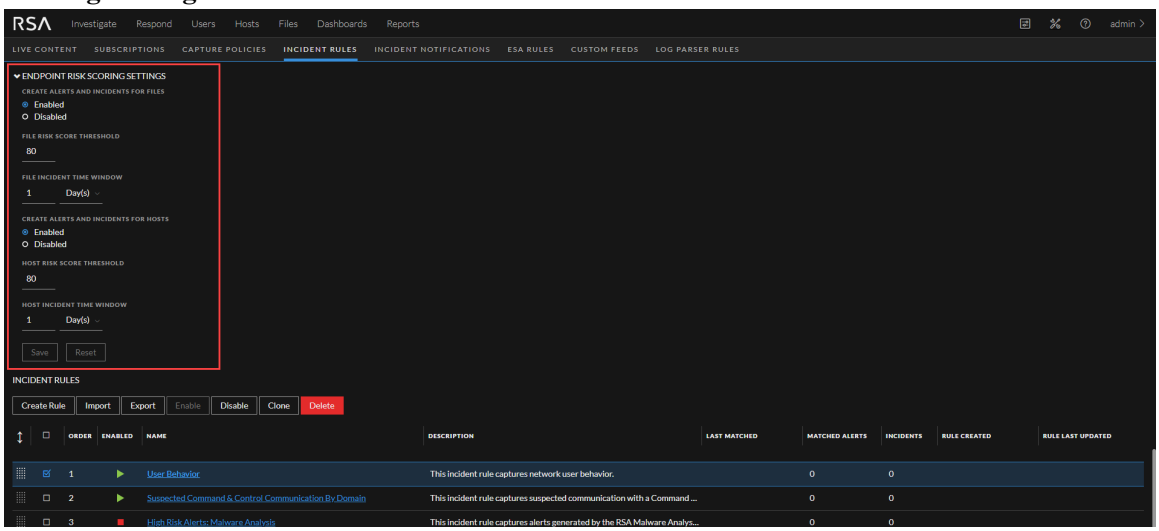
1. To access the Incident Rules view, go to  **(Configure) > Incident Rules**.



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

   - Endpoint Risk Scoring Settings
   - Incident Rules

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

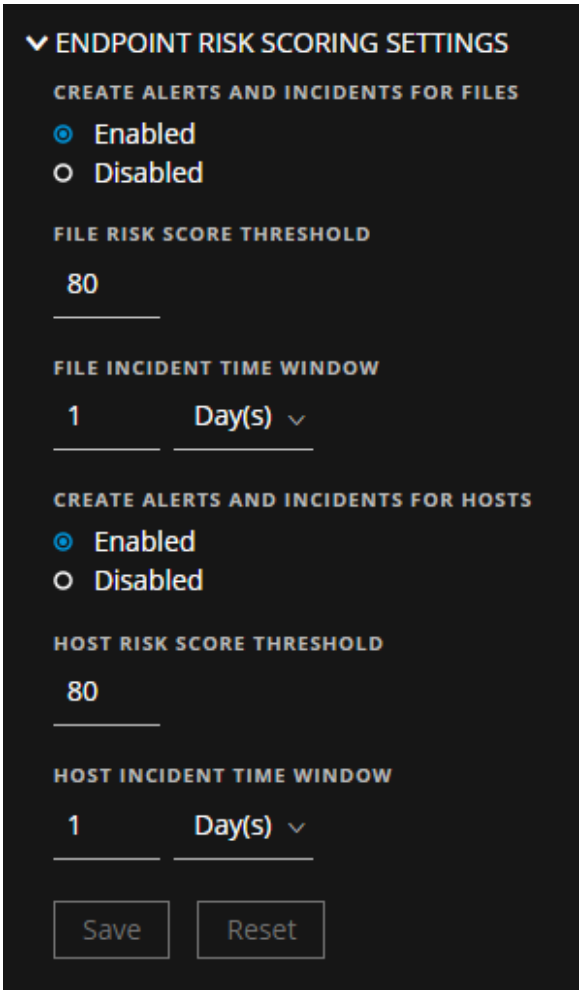


Endpoint Risk Scoring Settings

Note: Endpoint Risk Scoring Settings are available in NetWitness 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. NetWitness 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 *NetWitnesss Endpoint Configuration Guide*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.



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

Field / Button	Description
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. This option is enabled by default.

Field / Button	Description
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. 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. 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.
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, 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.
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. This option is enabled by default.
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. 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. 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.
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, 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.

Incident Rules

The Incident Rules section enables you to create and manage incident rules for automating the incident creation process. NetWitness 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 one or more rules in order to take an action, such as Enable or Export. You can select all rules by selecting the checkbox in the column header. You can only select one rule for the Clone or Delete actions.
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. 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 Set a 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 a Counter for Matched Alerts and Incidents.

Column	Description
Rule Created	Shows the date and time that the incident rule was created or imported.
Rule Last Updated	Shows the date and time that the incident rule was last updated.

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 incident rule.
Export button	(This option is available in NetWitness 11.4 and later.) Allows you to export one or more incident rules. This enables you to share incident rules with other NetWitness Servers on the same release version. The exported incident rules file is a ZIP file that contains two JSON files: one file contains the incident rules and the other file contains the incident rule schema. You cannot export Advanced incident rules; the export function only allows incident rules created using Rule Builder.
Import button	(This option is available in NetWitness 11.4 and later.) Allows you to import an incident rules ZIP file. This enables you to share incident rules with other NetWitness Servers on the same release version.
Enable button	(This option is available in NetWitness 11.4 and later.) Allows you to enable one or more rules from the incident rules list. You can also enable a rule in the Incident Rule Details view by selecting the Enabled checkbox in the Basic Settings section and then saving the rule.
Disable button	(This option is available in NetWitness 11.4 and later.) Allows you to disable one or more rules from the incident rules list. You can also disable a rule in the Incident Rule Details view by clearing the Enabled checkbox in the Basic Settings section and then saving the rule.
Clone button	Allows you to duplicate one incident rule at a time.
Delete button	Allows you to delete one incident rule at a time.
Name hyperlink	Allows you to edit an incident 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 NetWitness Version 11.1 and later.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure alert sources for the Respond view.	Step 1. Configure Alert Sources to Display Alerts in the Respond View
Administrator	Assign Respond view permissions.	Step 2. Assign Respond View Permissions
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*.

Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Related Topics

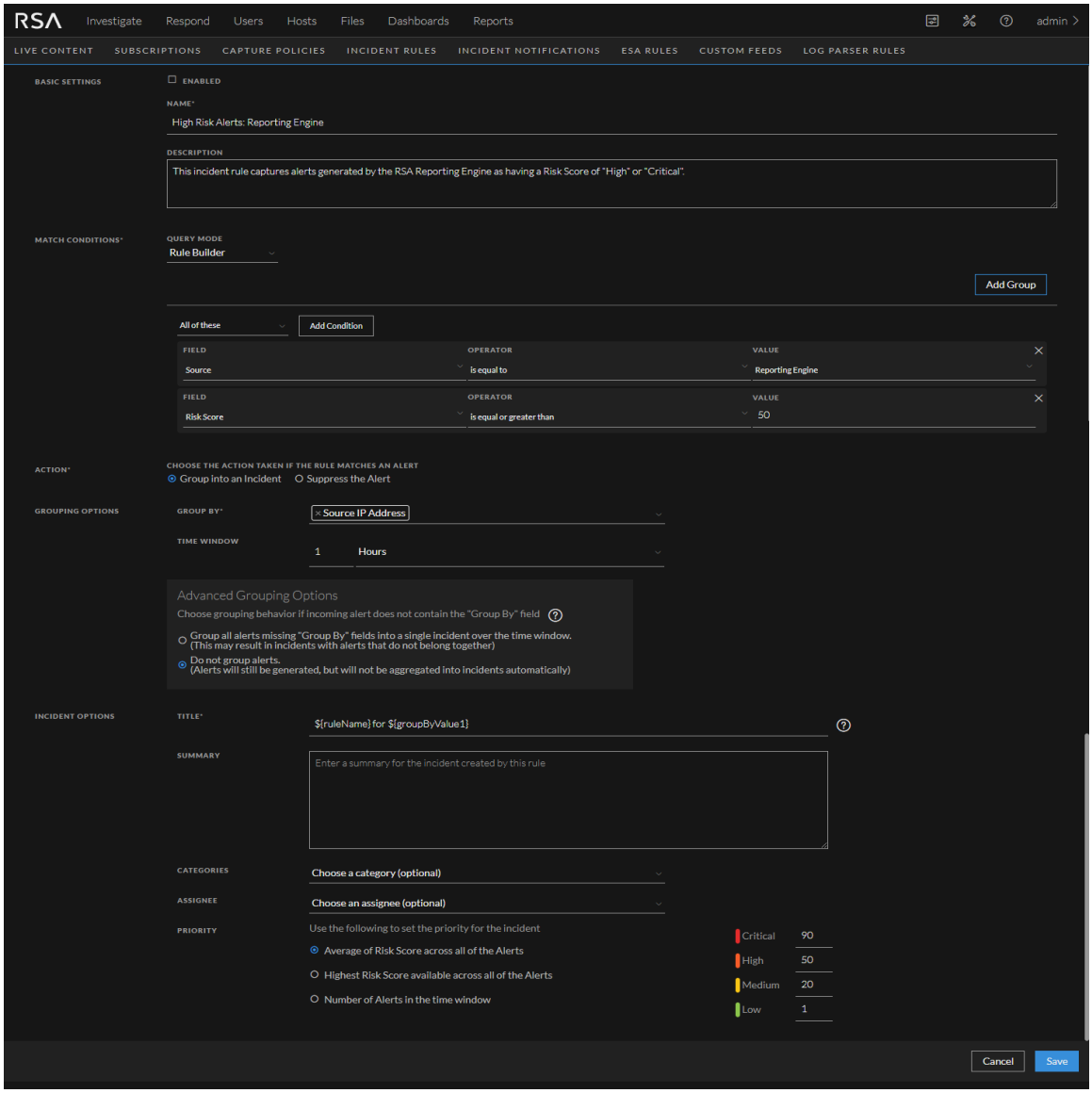
- Incident Rules View

Quick Look

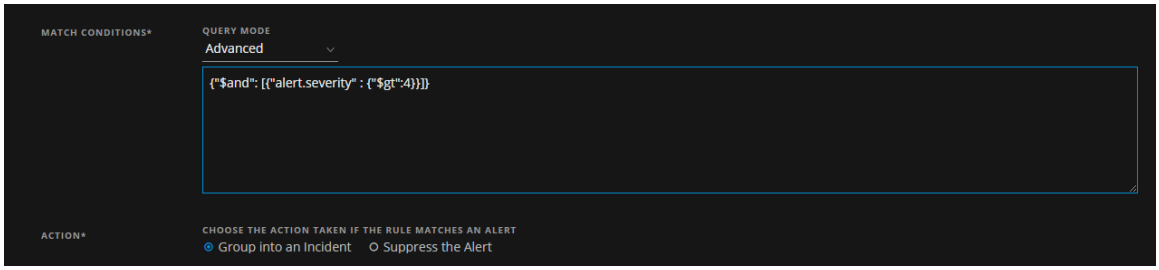
To access the Incident Rule Details view, do one of the following:

- 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 Settings	Enabled	Select to enable the rule.
	Name*	Name of the rule. *This is a required field.
	Description	A description of the rule to indicate which alerts get aggregated.
Match Conditions*	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/
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.

Section	Field	Description
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.
	Advanced Grouping Options	Alerts may sometimes come into Respond missing fields that are expected and used for aggregation into incidents (as defined by incident aggregation rules). This can be due to missing parsers, overly generic matching conditions, unexpected data sources, or log sources with unexpected formats. Choose how to handle alerts missing the fields required by the configured incident aggregation rules: • Automatically group them into a single incident over the configured time window. • Do not group them and manually include these orphaned alerts into an incident when required.

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
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

Incident Email Notification Settings View

The Incident Email 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 NetWitness 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 and go to the Servers tab or alternatively 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 Incident Email Notification Settings

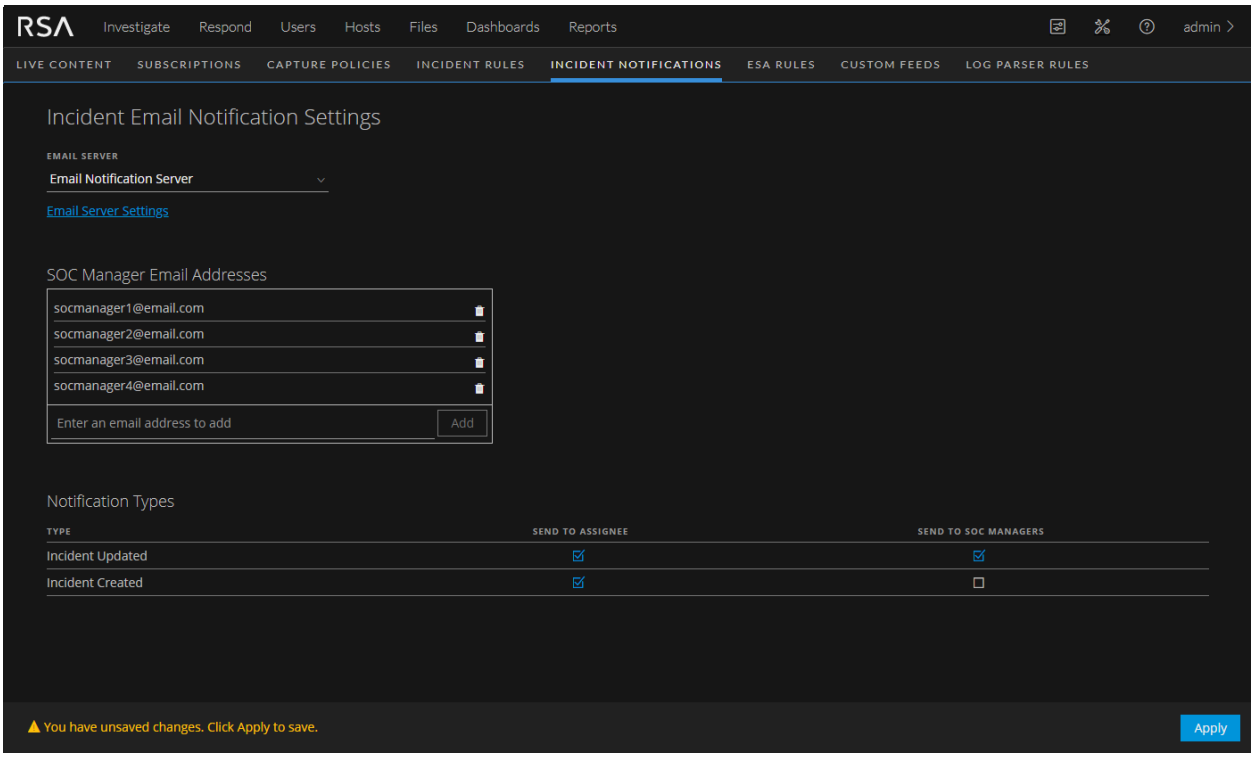
Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Related Topics

- Incident Rules View

Quick Look

To access the incident email notification settings, go to **(Configure) > Incident Notifications**.
The Incident Email Notification Settings view is displayed.



The following table lists the incident email 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. Configure the email server on the Servers tab. 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 the incident 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 (11.0 and earlier)

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

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

What do you want to do?

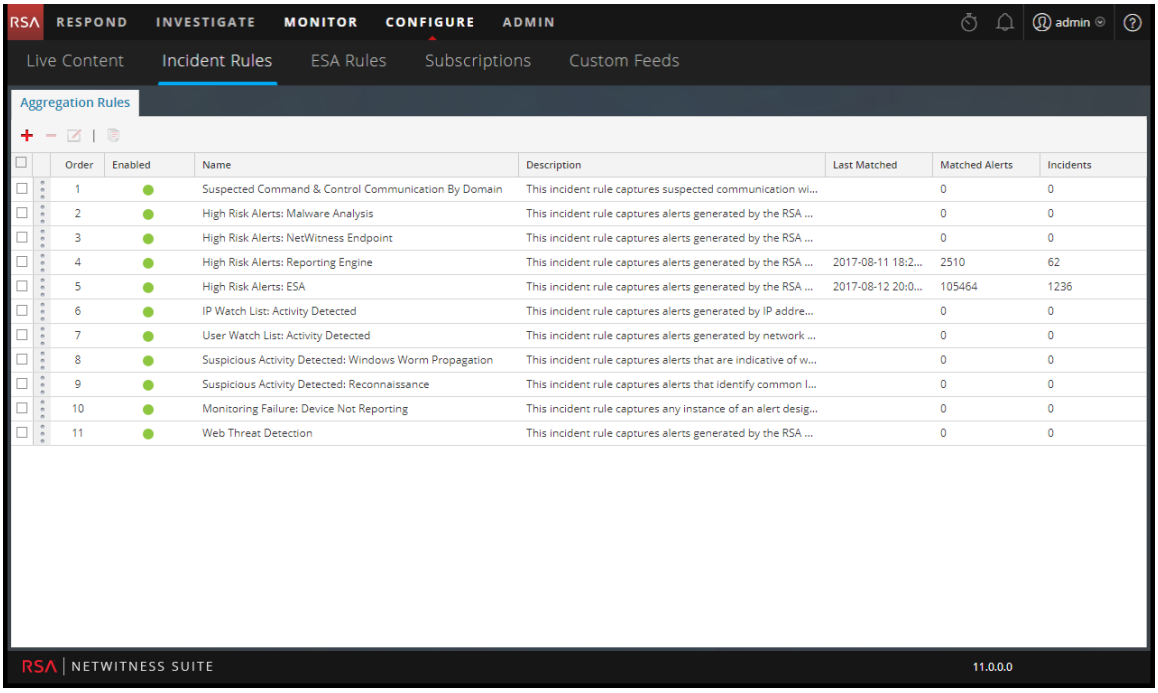
Role	I want to ...	Show me how
Analyst, Content Expert, SOC Manager	Create an aggregation rule.	Step 3. Enable and Create Incident Rules for Alerts
Incident Responders, Analysts, Content Experts, SOC Manager	View the results of my aggregation rule (View Detected Threats).	See "Responding to Incidents"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

Related Topics

- New Rule Tab (11.0 and earlier)

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 Set a 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 a 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 (11.0 and earlier)

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 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

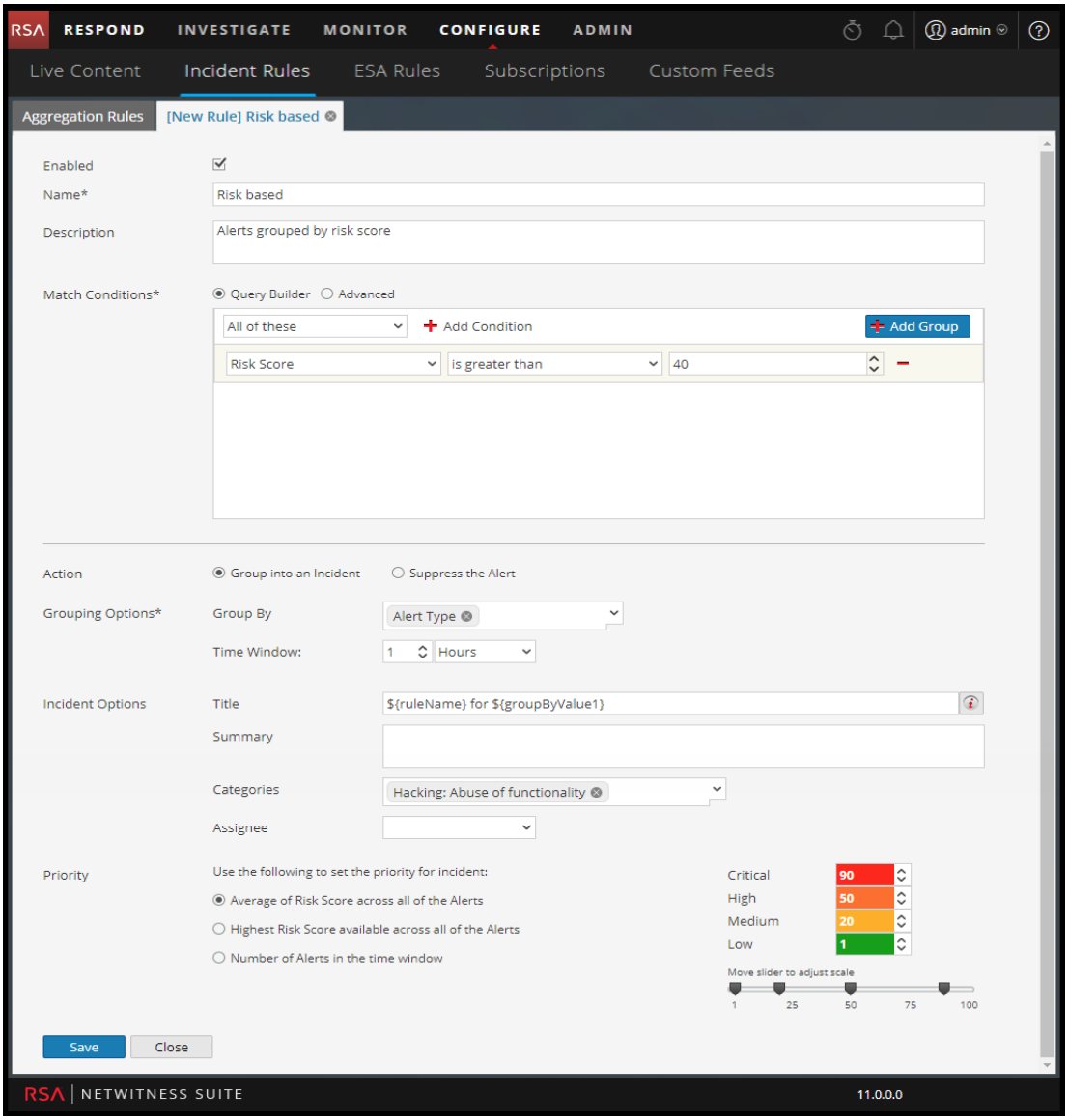
- Aggregation Rules Tab (11.0 and earlier)

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**.