

NetWitness[®] Platform

Version 12.5

NetWitness Response Actions Configuration Guide

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.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

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.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at <https://www.netwitness.com/standard-form-agreements/>.

© 2024 RSA Security LLC or its affiliates. All Rights Reserved.


September, 2024

Contents

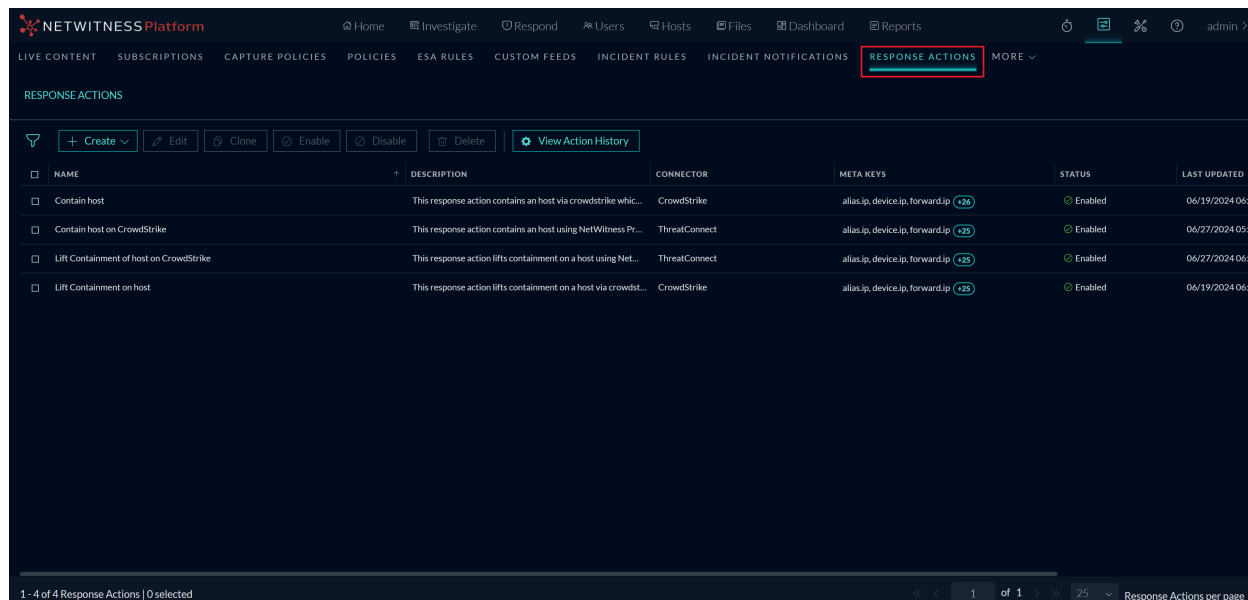
Response Actions	5
RBAC Permissions for Response Actions	6
Workflow	6
Response Actions Server	6
Integrate the Connector with NetWitness Platform	8
Support Connectors for NetWitness Platform	8
ThreatConnect	8
ThreatConnect Custom Actions	8
ThreatConnect Out-Of-The-Box Actions	11
CrowdStrike	14
Create and Manage Response Actions	16
Create Response Actions	16
Edit Response Actions	19
Clone Response Actions	21
Enable Response Actions	22
Disable Response Actions	22
Delete Response Actions	23
View Action History	24
Response Actions History View	26
Response Actions History Filters Panel	26
Response Actions History List	27
Response Actions History Overview panel	28
Quick Actions	29
Execute Quick Actions Option	29
Response Actions and Quick Actions Use Case Examples	32
Use Case #1: Managing Response Action and taking Quick Action in Respond view for the supported meta	32
Use Case #2: Taking Quick Action in Investigate view for the supported meta	37
Use Case #3: Taking Quick Action in Investigate view for the supported meta for OOTB Response Actions	37
Correlation between Response and Quick Actions	38
Quick Action History	40
Response Actions List view	41
Response Actions List	42
Response Actions Filters Panel	42

Response Actions Overview panel	43
Toolbar Actions in Response Actions view	43
Connect with Threat Connect using HTTPS	45
Establish HTTPS connection with SSL certificate verification	45
Establish HTTPS connection without SSL certificate verification	47
Troubleshooting	47
NetWitness Response Actions Reference Information	50
Response Actions View	51
Workflow	51
What do you want to do?	51
Related Topics	52
Quick Look	52
Response Actions List View	53
Response Actions Filters Panel	54
Response Actions Overview panel	55
Response Actions History List view	56
Response Actions History Filters Panel	57
Response Actions History Overview panel	59
Quick Actions Option	60
What do you want to do?	60
Related Topics	60
Quick Look	60
Quick Actions History View	62

Response Actions

Response Actions are the reactive operations performed on configured metas using NetWitness Orchestrator (ThreatConnect) or other third-party tools after triaging an event. The **ResponseActions** feature ( (CONFIGURE) > **More** > **Response Actions**) allows you to integrate the supported third-party tools or connectors with NetWitness platform and perform the following actions.

- Create and manage Response Actions for metas displayed in **Respond**, **Investigate**, **Hosts**, and **Users** views that support context highlights.
- Perform Quick Actions on the applicable meta and post the meta with additional information to the connector for taking further actions.



NAME	DESCRIPTION	CONNECTOR	META KEYS	STATUS	LAST UPDATED
Contain host	This response action contains an host via crowdstrike whic...	CrowdStrike	alias.ip, device.ip, forward.ip (+26)	Enabled	06/19/2024 06:
Contain host on CrowdStrike	This response action contains an host using NETWitness Pr...	ThreatConnect	alias.ip, device.ip, forward.ip (+25)	Enabled	06/27/2024 05:
Lift Containment of host on CrowdStrike	This response action lifts containment on a host using Net...	ThreatConnect	alias.ip, device.ip, forward.ip (+25)	Enabled	06/27/2024 06:
Lift Containment on host	This response action lifts containment on a host via crowdst...	CrowdStrike	alias.ip, device.ip, forward.ip (+25)	Enabled	06/19/2024 06:

There are four OOTB actions in the NetWitness Platform 12.5. CrowdStrike has two OOTB actions which are:

- **Contain host:** This response action allows you to isolate the host.
- **Lift Containment on host:** This response action allows you to unisolate the host.

ThreatConnect has two OOTB actions which are:

- **Contain host on Crowdstrike:** This response action allows you to isolate the host.
- **Lift Containment of host on Crowdstrike:** This response action allows you to unisolate the host.

Note: You cannot create, clone, and delete any of the out-of-the-box Response Actions created by default. You can only edit, disable, and enable them.

For more information on how to create and manage the Response Actions, see [Create and Manage Response Actions](#). For more information on how to add parameters and post the parameters with meta to the connector, see [Response Actions and Quick Actions Use Case Examples](#).

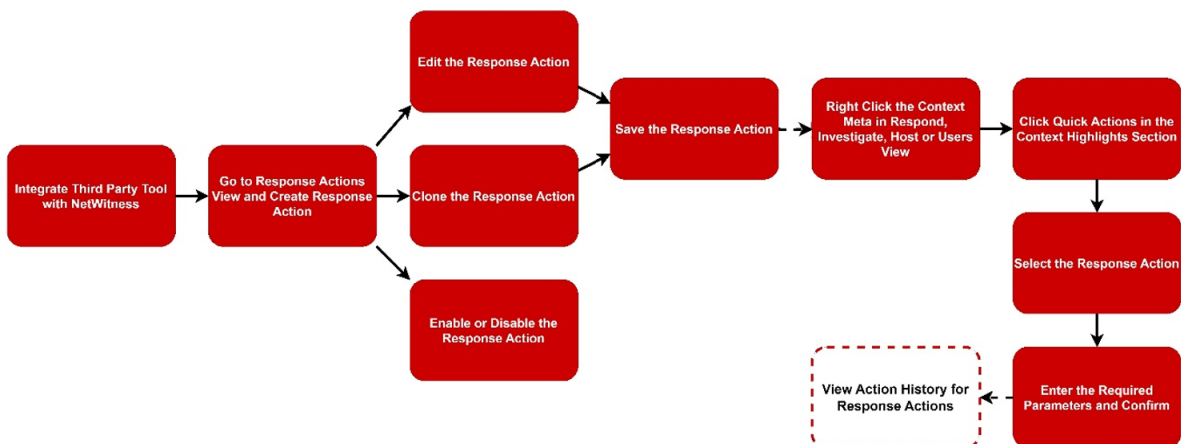
RBAC Permissions for Response Actions

- You can view the Response Actions configured in the **Response Actions** view only if you have **response-actions-server.actiondefinition.read** permission.
- You must have **response-actions-server.actiondefinition.manage** permission to create, edit, clone, delete, enable, and disable the Response Action.
- You must have **response-actions-server.history.read** permission to view the Response Action history.
- You must have **response-actions-server.actiondefinition.execute** permission to execute any response actions.

For more information, see **How Role-Based Access Control Works** topic in the [System Security and User Management Guide](#).


Workflow

The following figure shows the high-level NetWitness Response Actions workflow process.



For more information on the workflow, see [Response Actions and Quick Actions Use Case Examples](#).

Response Actions Server

The service **Response Actions Server** is introduced in the  **Admin > Hosts** view to integrate the third-party tools with NetWitness Platform.

NetWitness Response Actions Configuration Guide

The screenshot shows the NetWitness console interface. The top navigation bar includes: HOSTS, SERVICES, EVENT SOURCES, ENDPOINT SOURCES, HEALTH & WELLNESS, SYSTEM, and SECURITY. The main content area is divided into two panes. The left pane, titled "Groups", shows a list with "All" selected. The right pane, titled "Hosts", displays a table of hosts and a "Services" dropdown menu.

Hosts Table:

Name	Host	IP	Services	Current Version	Update Version	Status
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	Up-to-Date
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	Up-to-Date
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	Up-to-Date
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	Up-to-Date
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	Up-to-Date
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	Up-to-Date

Services Dropdown Menu:

- Admin Server
- Broker
- Config Server
- Content Server
- Integration Server
- Investigate Server
- License Server
- Orchestration Server
- Reporting Engine
- Respond Server
- Response Actions Server** (highlighted with a red box)
- Security Server
- Source Server

Page 1 of 1 | Displaying 1 - 6 of 6

Integrate the Connector with NetWitness Platform

You must integrate the connector with NetWitness Platform before creating a Response Action. The meta and the additional parameters information can be forwarded to the connector through NetWitness Platform only when you integrate the connector with NetWitness Platform.

Support Connectors for NetWitness Platform

Version	Connector Type	Actions Type
12.4 and later	ThreatConnect	Custom Actions
12.5 and later	ThreatConnect	OOTB Actions to CrowdStrike
12.5 and later	CrowdStrike	OOTB Actions

ThreatConnect



You can perform the following actions using the ThreatConnect connector type.

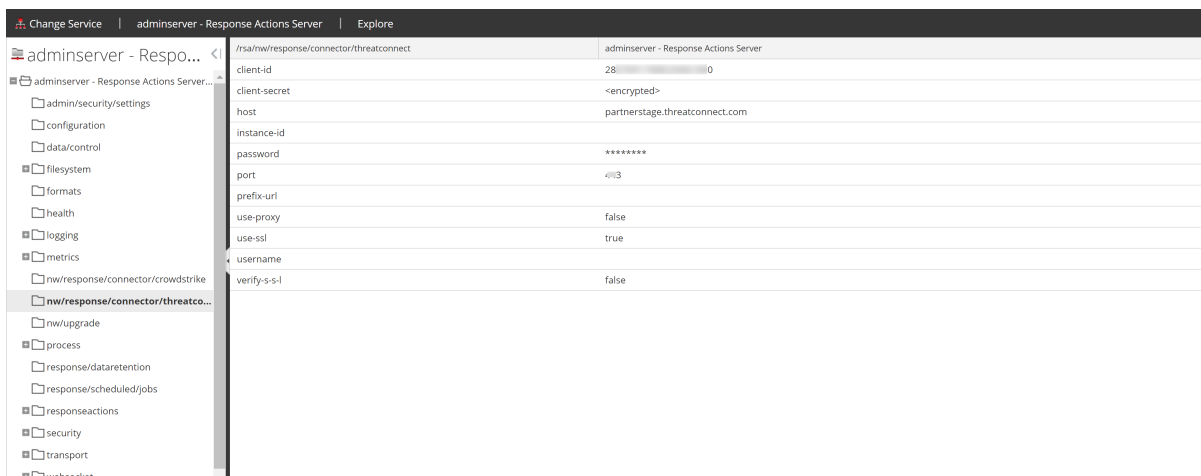
- [ThreatConnect Custom Actions](#)
- [ThreatConnect Out-Of-The-Box Actions](#)

ThreatConnect Custom Actions

The following section explains how to integrate a connector such as ThreatConnect with the NetWitness Platform.

To integrate ThreatConnect with NetWitness Platform

1. Go to  (Admin) > Services.
2. Select the **Response Actions Server** service in the **Services** view and go to  > **View** > **Explore**.
The Response Actions Server Explore view is displayed.



3. Select **nw/response/connector/threatconnect** in the left panel.

4. Enter the following information:

- **client-id**: This field can be left blank as it is unnecessary for this integration.
- **client-secret**: This field can be left blank as it is unnecessary for this integration.
- **host**: Provide the Host IP or domain name of ThreatConnect instance. In case of ThreatConnect, the Host IP is the IP displayed in the URL of ThreatConnect Playbook's Webhook Trigger.
- **instance-id**: If `playbookWebHookPathByOrg` is enabled in ThreatConnect, you must enter the Organization ID as the **instance-id** in the Response Actions Server Explore view. If `playbookWebHookPathByOrg` is not enabled, leave this field empty.

For example: If you enter **api/playbook/1/blockipaddress** in the **Path** field in ThreatConnect Playbook's Webhook Trigger, you should enter **1** in the **instance-id** field.

- **prefix-url**: This is the prefix part of the **Path** field in ThreatConnect Playbook's Webhook Trigger. You must enter the prefix part as the `prefix-url` in Response Actions Server Explore view.

For example: If you enter **api/playbook/blockipaddress** in the **Path** field in ThreatConnect Playbook's Webhook Trigger, you should enter **api/playbook/** in the **prefix-url** field.

- **username**: Enter the ThreatConnect Playbook's Webhook Trigger username if authentication is enabled.
- **password**: Enter the ThreatConnect Playbook's Webhook Trigger password if authentication is enabled.

Note: All the ThreatConnect Playbook's Webhook Trigger must have the same username and password when used by NetWitness Platform.

- **port**: Enter the ThreatConnect Playbooks port.

Note: By default, ThreatConnect Playbook Webhook uses the port 443 to accept request.

- **use-ssl**: Set this field to **true** to enable SSL.
- **verify-s-s-l**: Set this field to **true** to enable SSL verification.

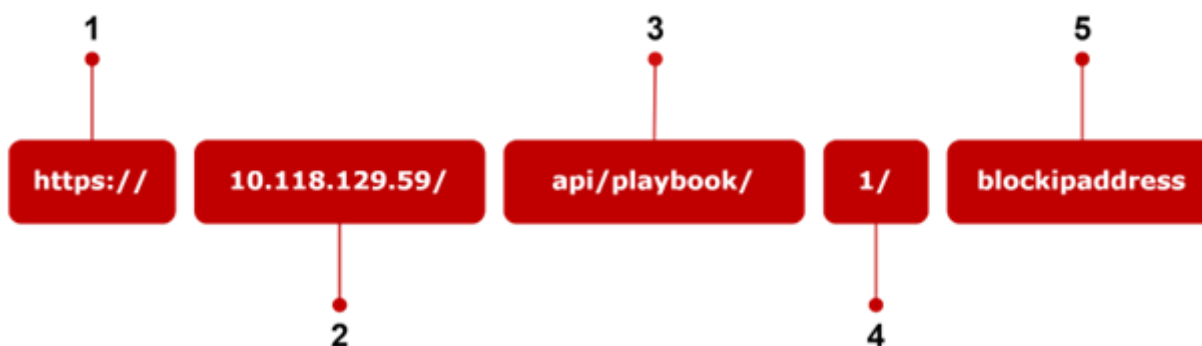
Note: This will require a certificate that is issued and configured.

- **use-proxy:** Set this field to **true** to enable proxy.

The following diagram explains the URL structure associated with ThreatConnect Playbook's Webhook Trigger.

Parts of URL Structure

Example: `https://10.118.129.59/api/playbook/1/blockipaddress`



The following table explains the parts of the URL structure associated with ThreatConnect Playbook's Webhook Trigger.

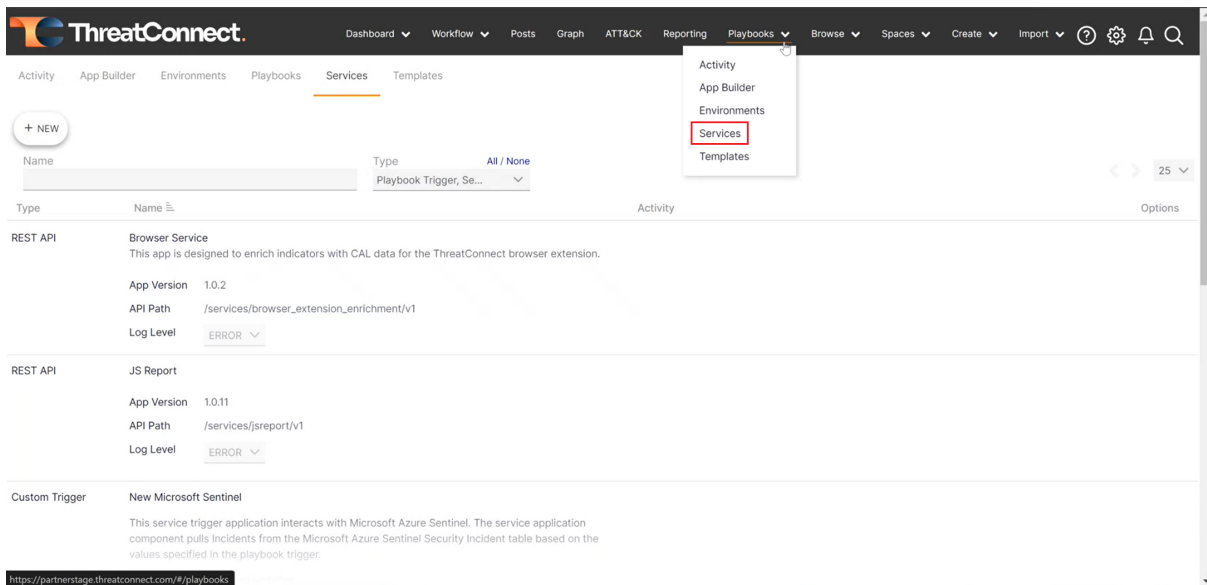
Sl.no	Description
1	This part provides information about the SSL or non-SSL connection established between NetWitness Platform and ThreatConnect instance. For example: If the SSL connection is established between NetWitness Platform and ThreatConnect, this part displays https .
2	This part provides information about the Host IP or domain name of ThreatConnect instance.
3	This part provides information about the prefix-url associated with ThreatConnect Playbook's Webhook Trigger. For example: api/playbook/
4	This part of the URL provides information about the instance-id associated with ThreatConnect Playbook's Webhook Trigger. For example: 1
5	This part of the URL provides information about the URL Path associated with ThreatConnect Playbook's Webhook Trigger. For example: In the above diagram, blockipaddress is the URL Path associated with ThreatConnect Playbook's Webhook Trigger. The URL Path associated with ThreatConnect Playbook's Webhook Trigger must be entered while creating and managing Response Actions.

ThreatConnect Out-Of-The-Box Actions

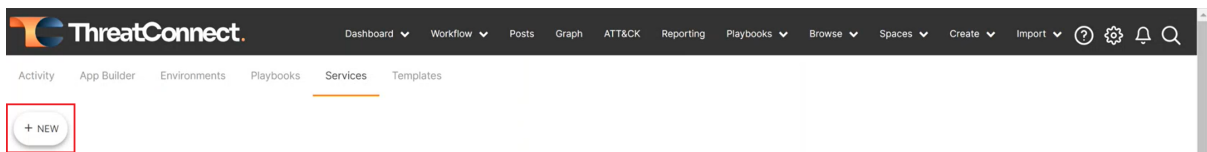
The following section explains how to integrate a connector such as CrowdStrike with the NetWitness Platform through ThreatConnect.

Create NetWitness Response Actions Proxy Service in ThreatConnect for Supported Connectors

1. Register and Sign in to ThreatConnect.
2. Generate the **Client ID** and **Client Secret** which shall be used for the configuration of Response Actions on the NetWitness Platform.
3. In the **Playbooks** dropdown, click **Services**.



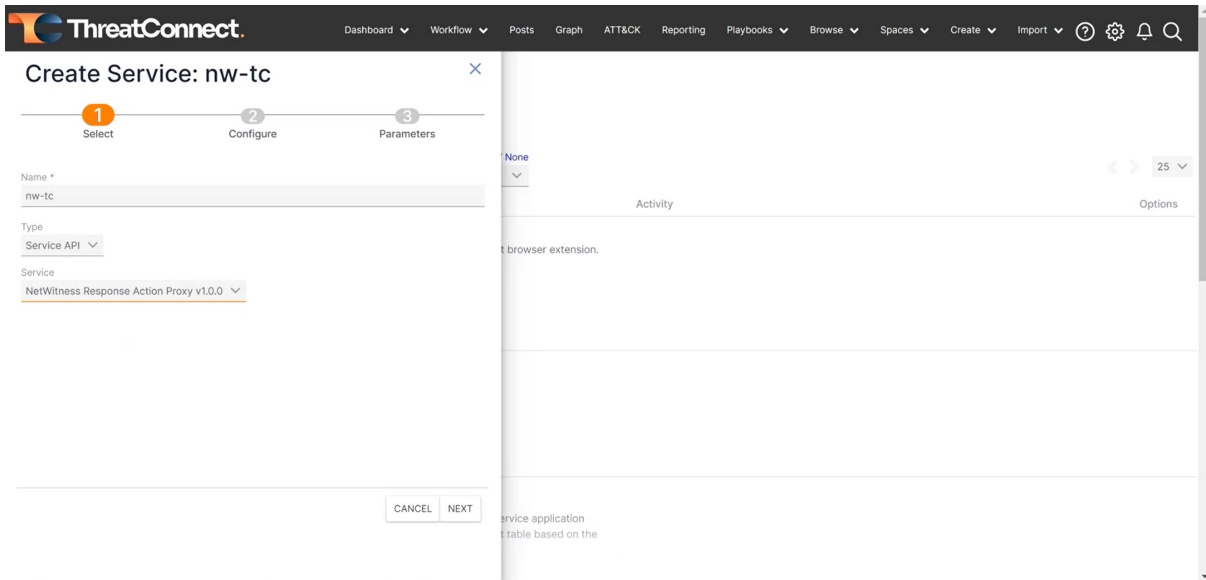
4. Click **+NEW** to create a Service.



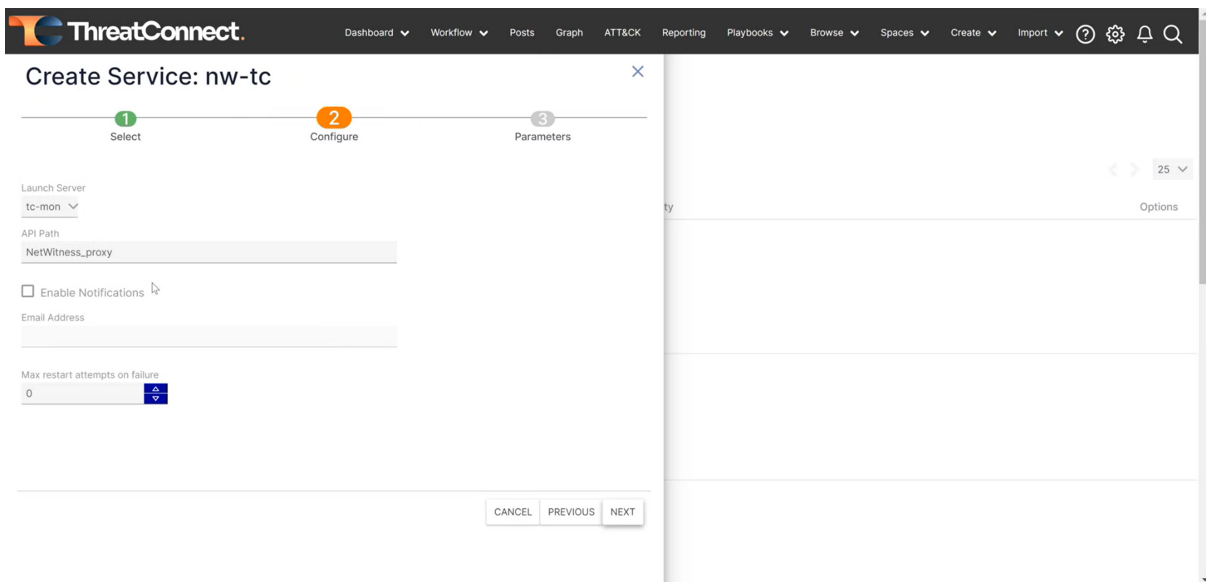
5. Enter any name in the **Name** field.

Note: The name entered will reflect in front of the **Create Service** field at the top.

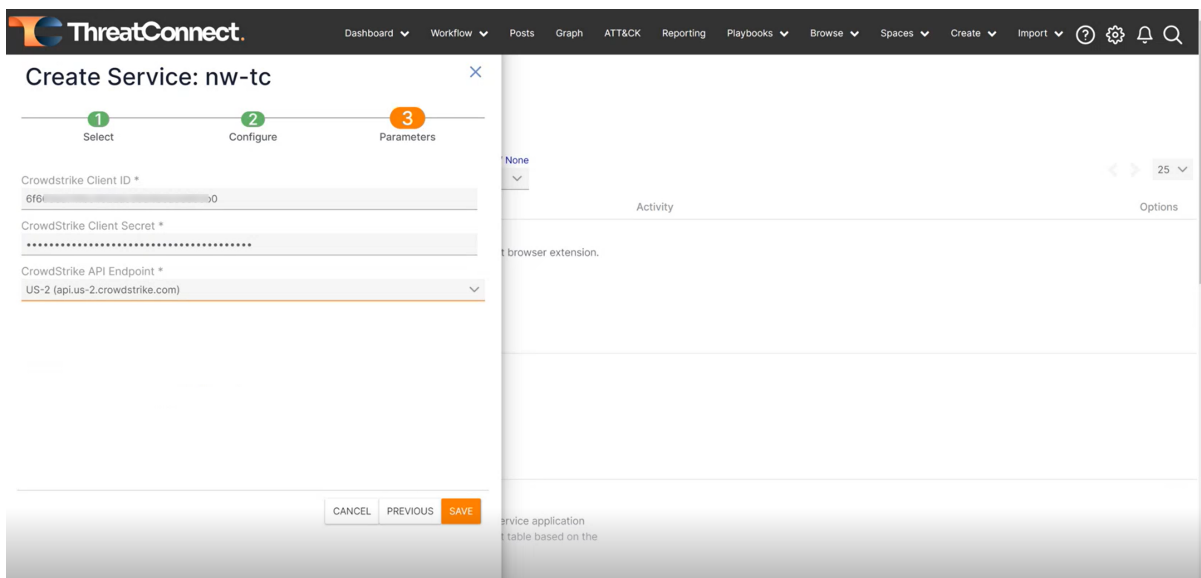
6. From the **Service Type** drop-down, select **Service API**.
7. From the **Service** dropdown, scroll and select **NetWitness Response Action Proxy** from the list of available services.



8. Click **Next** to fill the **Configuration** details.
9. In the **Configure** tab, by default the **Launch Server** is set to **tc-mon** and the **API Path** is set to **NetWitness_proxy**.

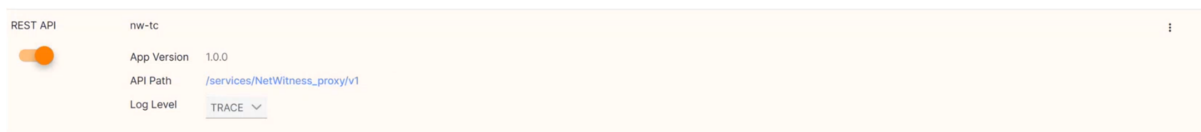


10. Click **Next** to enter the setup parameters.
11. In the **Parameters** tab, enter the **Crowdstrike Client ID** and **Crowdstrike Client Secret**.





- Click **Save**, a new Service is created.

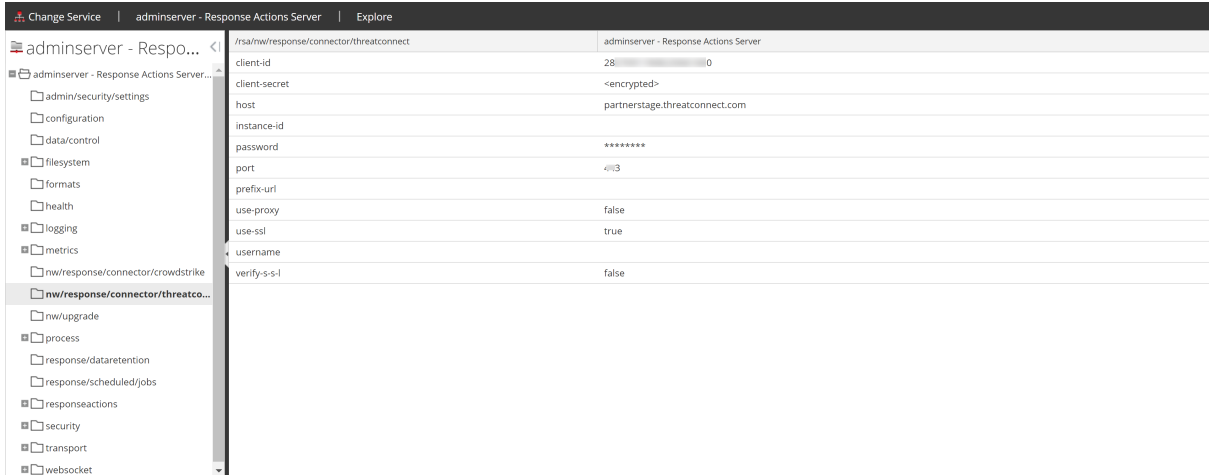
Note: After a new Service is created, the **Rest API** for the newly created Service will be in disabled mode. Click the toggle button to enable the **Rest API**.



This API path is required in the Response Action's **Service API Path** in the NetWitness Platform. The Service is now ready to accept the request from NetWitness and perform any action.

To integrate CrowdStrike with NetWitness Platform through ThreatConnect

- Go to  (**Admin**) > **Services**.
- Select the **Response Actions Server** service in the **Services** view and go to  > **View** > **Explore**. The Response Actions Server Explore view is displayed.



3. Select **nw/response/connector/threatconnect** in the left panel.
4. Enter the following information:
 - **client-id**: Enter the client-id generated by ThreatConnect.
 - **client-secret**: Enter the client-secret generated by ThreatConnect.
 - **host**: Provide the Host IP or domain name of ThreatConnect instance.
 - **instance-id**: This field can be left blank as it is unnecessary for this integration.
 - **password**: This field can be left blank as it is unnecessary for this integration.
 - **port**: Enter the ThreatConnect instance port.

Note: By default, ThreatConnect instance uses the port 443 to accept request.



- **prefix-url**: This field can be left blank as it is unnecessary for this integration.
- **use-proxy**: Set this field to **true** to enable proxy.
- **use-ssl**: Set this field to **true** to enable SSL.
- **username**: This field can be left blank as it is unnecessary for this integration.
- **verify-s-s-l**: Set this field to **true** to enable SSL verification.

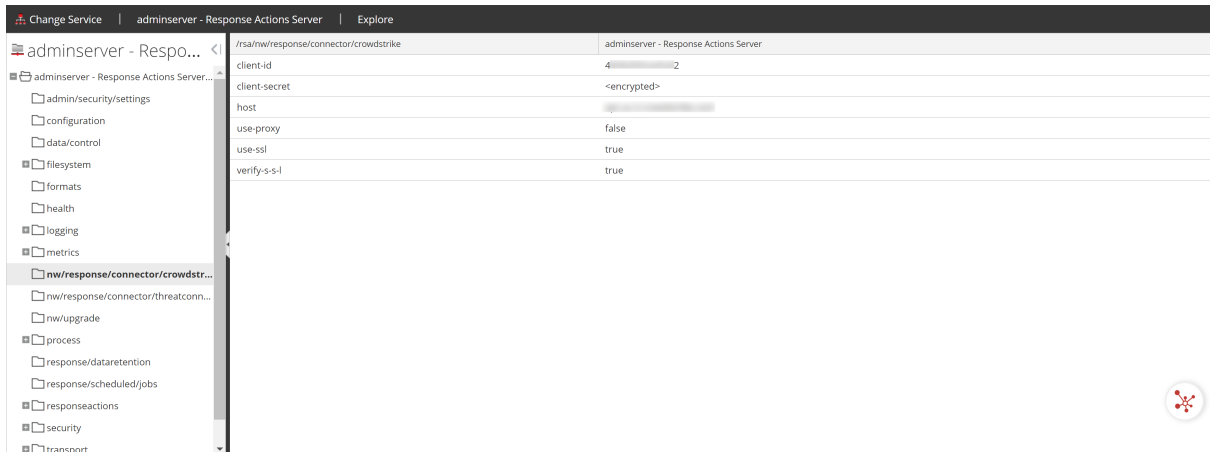
Note: This will require a certificate that is issued and configured.

CrowdStrike

The following section explains how to integrate a connector such as CrowdStrike with the NetWitness Platform.

To integrate CrowdStrike with NetWitness Platform

1. Go to  (Admin) > Services.
2. Select the **Response Actions Server** service in the **Services** view and go to  > **View** > **Explore**. The Response Actions Server Explore view is displayed.



3. Select **nw/response/connector/crowdstrike** in the left panel.
4. Enter the following information:
 - **client-id**: Enter the client-id generated by CrowdStrike.
 - **client-secret**: Enter the client-secret generated by CrowdStrike.
 - **host**: Provide the Host IP or domain name of CrowdStrike instance.
 - **use-proxy**: Set this field to **true** to enable proxy.
 - **use-ssl**: Set this field to **true** to enable SSL.
 - **verify-s-s-l**: Set this field to **true** to enable SSL verification.


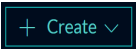
Note: This will require a certificate that is issued and configured.

Create and Manage Response Actions


The **Response Actions** view allows you to create the new Response Actions and manage the existing Response Actions. You can perform the following actions using the **Response Actions** view.

- [Create Response Actions](#)
- [Edit Response Actions](#)
- [Clone Response Actions](#)
- [Enable Response Actions](#)
- [Disable Response Actions](#)
- [Delete Response Actions](#)

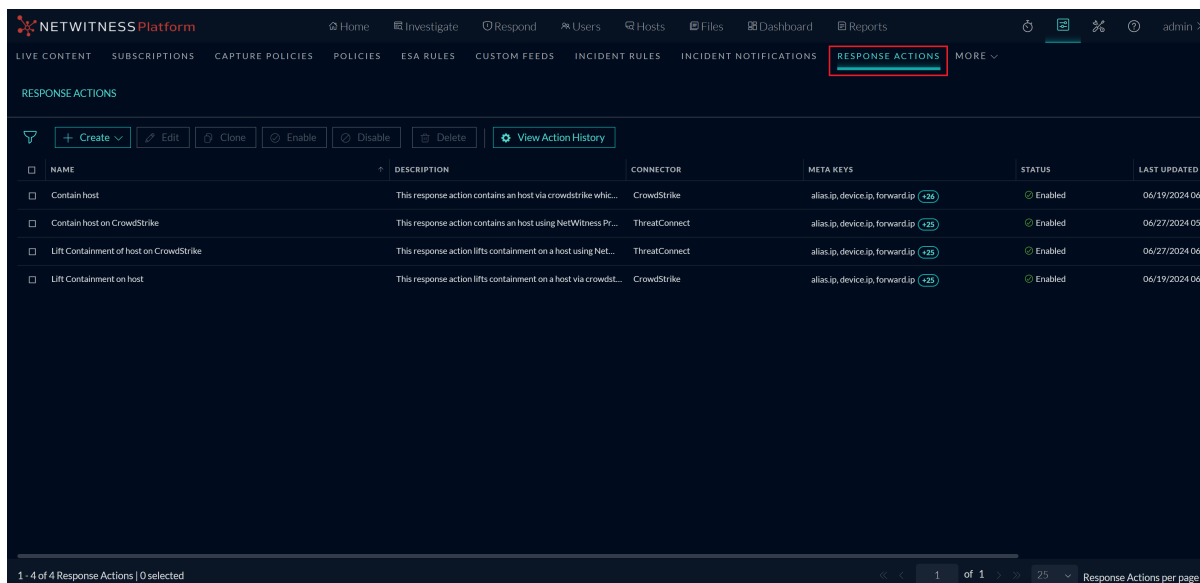
Create Response Actions

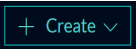
You can create the Response Action for any meta in the **Create Response Action** view ( (CONFIGURE) > More > Response Actions >  > Create Response Action).

To create custom Response Actions

1. Go to  (CONFIGURE) > More > Response Actions.

The **Response Actions** view is displayed.



2. Click  and select the connector from the drop-down list.

The **Create Response Action** view is displayed.

3. Enter the Action name for the Response Action.

For example: If the Response Action is to block an IP address associated with the context meta, you can enter Block IP or Block IP Address as the Action name in the **Action Name** field.

4. Enter the description of the Response Action being created.

For example: You can enter Creating this **Response Action to block the IP address** in the **Description** field.

5. Enter the meta keys of the applicable metas on which you want to perform the Response Action.

For example: If the meta keys are **ip_address**, **ip.src**, and **mac_address**, you must enter **ip_address**, **ip.src**, **ip_src**, and **mac_address** in the **Applicable Meta** field.

Note: Enter the comma-separated values in the **Applicable Meta** field. If any meta key is available in multiple formats, you must enter the multiple formats of the meta key in the **Applicable Meta** field.

For example: If a meta key **user.src** is also available in the form of **user_src**, you must enter both **user.src** and **user_src** formats in the **Applicable Meta** field.

6. Enter the **URL Path** you used while creating the webhook trigger in the ThreatConnect playbook for NetWitness Platform, in the **URL Path** field.

For more information, see [Integrate the Connector with NetWitness Platform](#).

7. Click + **Add Parameter** option next to the Parameters field.

The **Add Parameter** window is displayed.

8. Provide the following information.

- **Parameter Key:** Enter the key name of the key-value pair that you want to forward to the connector. This key name is also displayed in the **Response Actions Overview panel**.

Note: If you turn on the toggle for **Default Parameter**, the selected NetWitness meta value will be associated with this key. It is mandatory to have at least one key marked as a Default Parameter.

IMPORTANT: You must not enter the following reserved parameter keys in the **Parameter Key** field.

- nw-user
- nw-comment
- nw-actionId
- nw-actionName

- **Parameter Type:** Select any of the following format types. You must select any of these types on the basis of the parameter value that you want to forward to the connector. Basic input validations are made based on the chosen type.
 - **Number:** Select this option if you want to forward a numerical parameter type to the connector.
 - **String:** Select this option if you want to forward a string parameter type to the connector.
 - **Email:** Select this option if you want to forward an email parameter type to the connector.
 - **IP:** Select this option if you want to forward IPv4 type to the connector.

- **Parameter Label:** Enter the label or field name of the parameter as it appears in the **Quick Actions** window form, that you want to forward to the connector.

For example: If you want to forward the IP 10.124.85.29 to the connector for blocking it, you can enter **Block IP Address** as the label in the **Parameter Label** field.

Note: While performing the **Quick Actions** on the applicable meta, this label will be displayed as a field in the **Quick Actions** window. In this field, you must enter the required data to be forwarded to the connector for further processing. For more information, see [Quick Actions](#). Parameter Key will be used only in the backend to send the key-value pair information.

- **Parameter Placeholder:** Enter the placeholder text that can be used as a hint in the form field while filling up the Quick Action form on the applicable meta.

For example: If you enter **Block IP Address** as the value in the **Parameter Label** field and **Additional IP** as the text in the **Parameter Placeholder** field, the text **Additional IP** will be displayed as the placeholder text in the Quick Actions window under the **Block IP Address** field.


Note: By default, the toggle for **Default Parameter** is turned off. When you turn on the toggle for **Default Parameter**, the fields **Parameter Type**, **Parameter Label**, and **Parameter Placeholder** will be grayed out. You must enter the required information in the fields that are marked with *. For more information on how to add parameters and send the parameters to the connector, see [Response Actions and Quick Actions Use Case Examples](#).

9. Click **Add**.
10. Click **Save Action**.

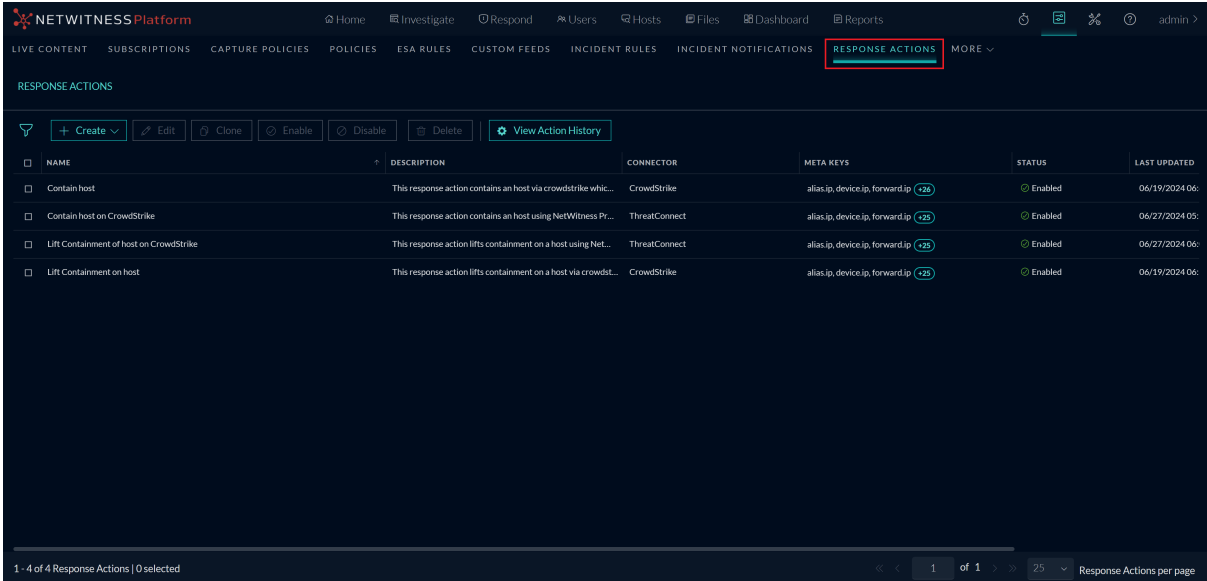
Edit Response Actions

You can edit an existing Response Action displayed in the **Response Actions** view and modify the Action Name, Action Description, supported metas, and URL Path associated with the connector.

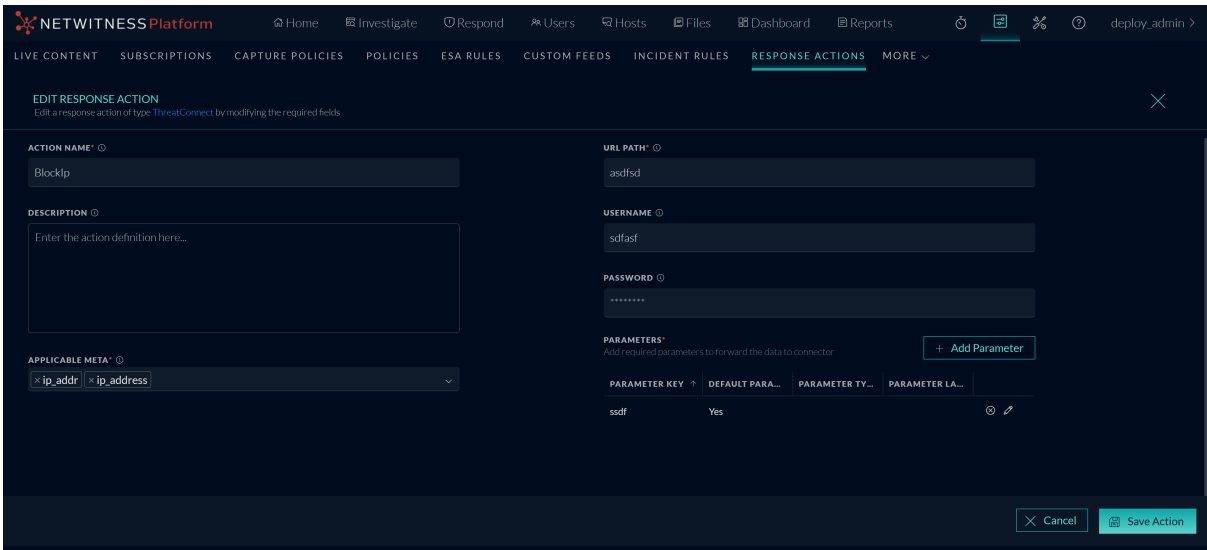
To edit the Response Action

1. Go to  (CONFIGURE) > **More** > **Response Actions**.

The **Response Actions** view is displayed.

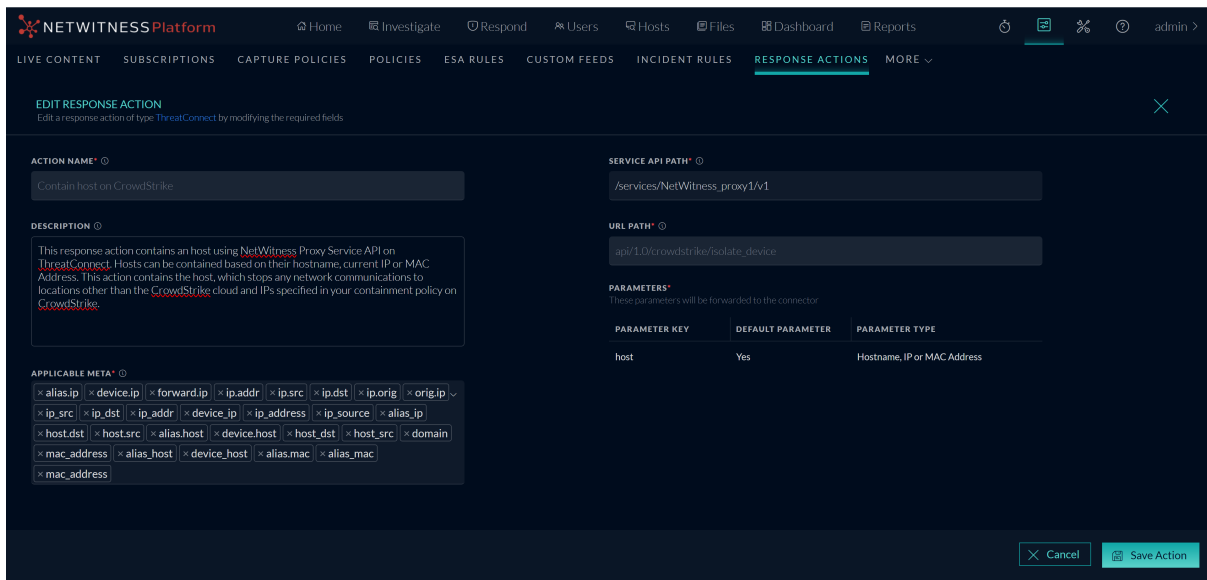


2. Select the Response Action and click **Edit**.
The **Edit Response Action** view is displayed.



Note: For CrowdStrike, you can only modify the **Description** and **Applicable Meta** fields while editing the Response Actions.

Note: For CrowdStrike integrating through ThreatConnect, the fields do not require changes. You can only modify the **Description**, **Applicable Meta** and **Service API** fields while editing the Response Actions. Copy the Service API path from the ThreatConnect Service and replace it here, if necessary.




3. Modify the required fields.
4. Click **Save Action**.

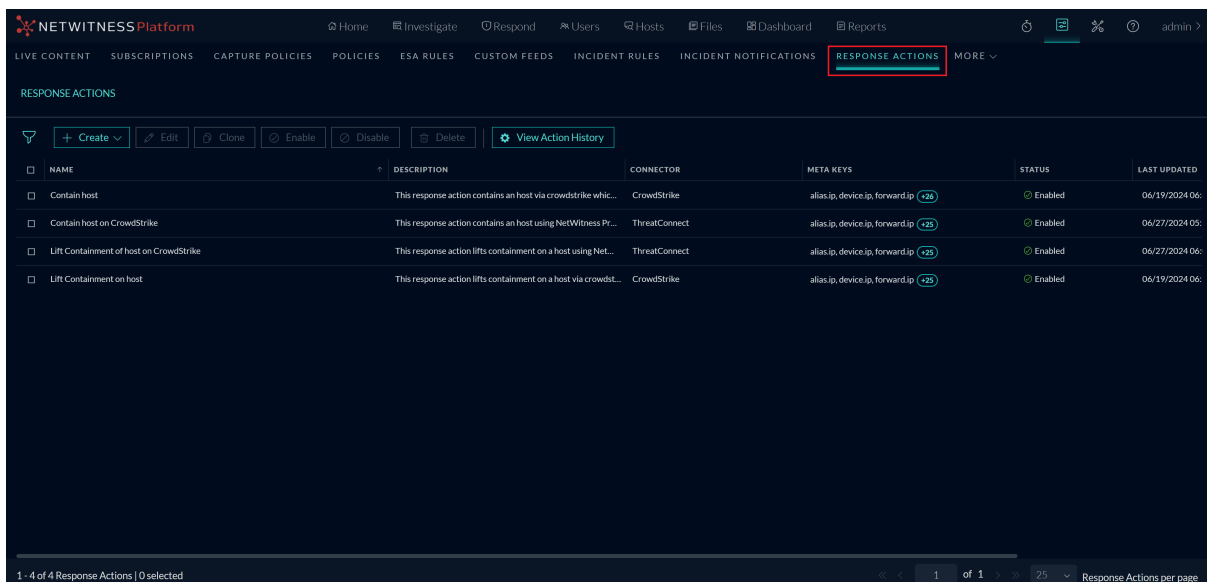
Clone Response Actions

You can clone an existing Response Action to re-use certain data and modify certain fields in the cloned Response Action.

To clone the Response Action

1. Go to  (CONFIGURE) > **More** > **Response Actions**.

The **Response Actions** view is displayed.



2. Select the Response Action and click **Clone**.


The **Create Response Action** view is displayed.

3. Modify the existing data as per your preference and click **Save Action**.

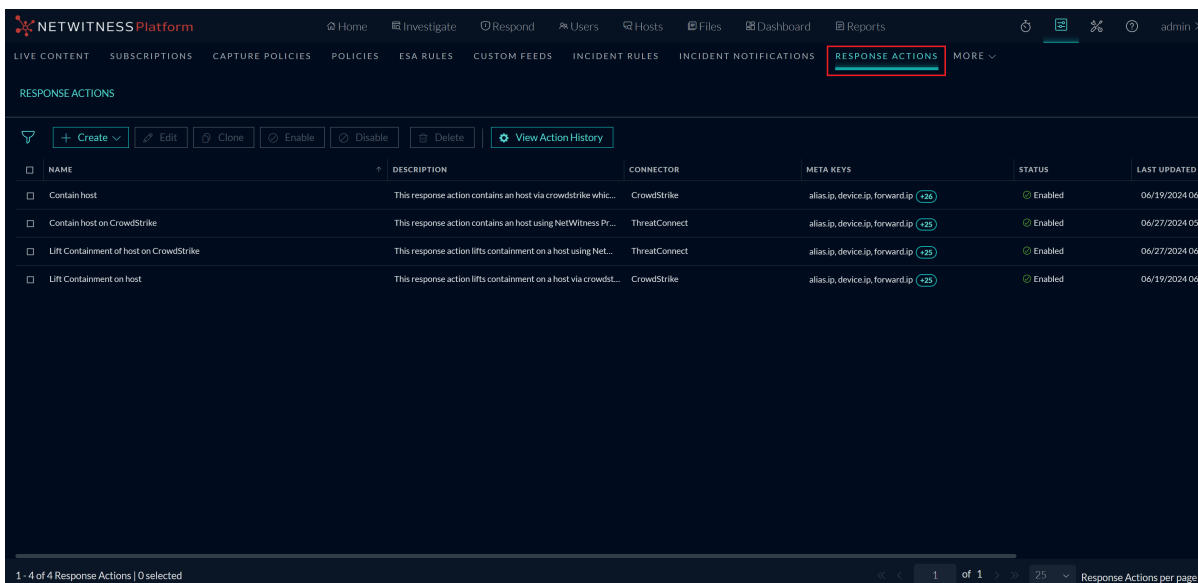
Enable Response Actions

You can enable the disabled Response Action in the **Response Actions** view.

To enable the Response Action

1. Go to  (CONFIGURE) > **More** > **Response Actions**.

The **Response Actions** view is displayed.




2. Select the disabled Response Action and click **Enable**.

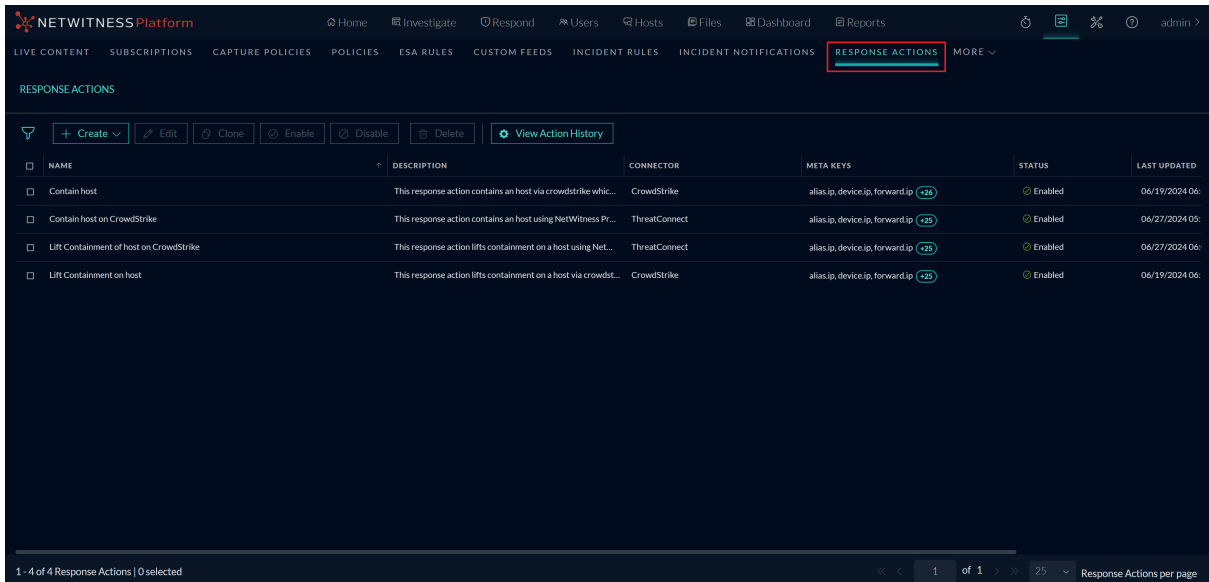
Disable Response Actions

You can disable any Response Action which is in the enabled state in the **Response Actions** view.

To disable the Response Action

1. Go to  (CONFIGURE) > **More** > **Response Actions**.

The **Response Actions** view is displayed.



2. Select the enabled Response Action and click **Disable**.

Note: The disabled Response Actions will not be populated in the **Quick Actions** window for selection.

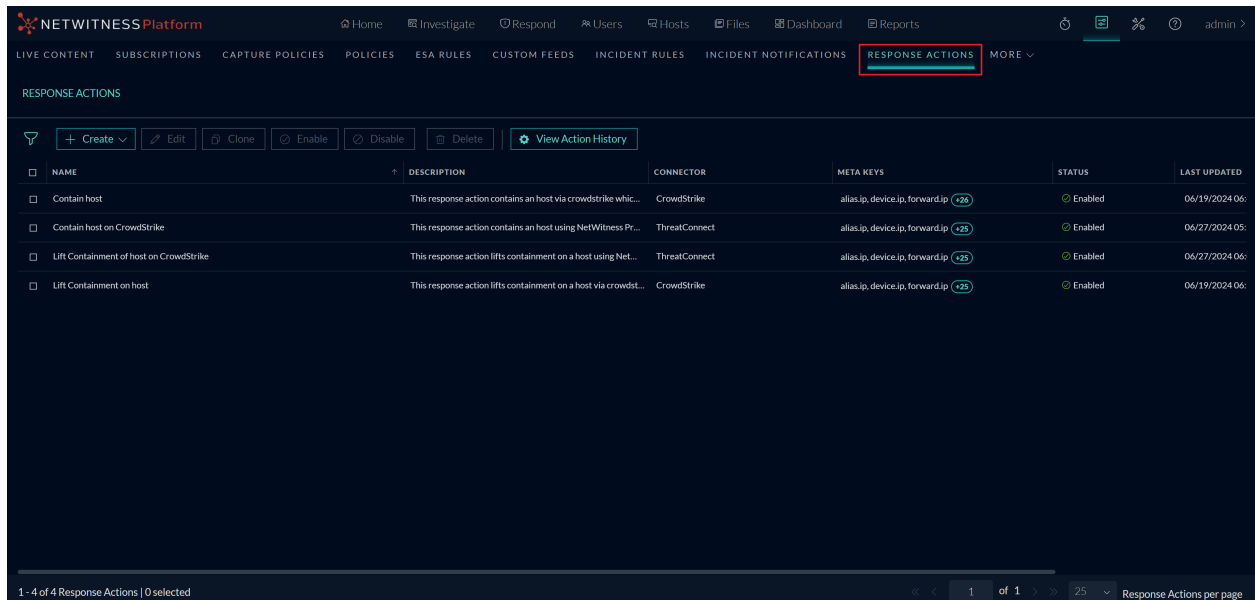
Delete Response Actions

You can delete any unwanted Response Action in the **Response Actions** view.

To delete the Response Action


1. Go to **(CONFIGURE) > More > Response Actions**.

The **Response Actions** view is displayed.




2. Select the Response Action you want to delete and click **Delete**.

View Action History

When you execute **Response Actions** in the Quick Actions, the actions performed are recorded and the associated data is displayed in the Response Actions History view ( (CONFIGURE) > **More** > **Response Actions** > **View Action History** > **Response Actions History**). This is a global view of all actions performed across all Response actions.

EXECUTED ON	NAME	CONNECTOR	META KEY	META VALUE	STATUS	EXECUTED BY
06/27/2024 06:06:11 am	Lift Containment of host on CrowdStrike	ThreatConnect	ip_address		Success	deploy_admin
06/27/2024 06:05:22 am	Lift Containment of host on CrowdStrike	ThreatConnect	ip_address		Success	deploy_admin
06/27/2024 05:40:16 am	Contain host on CrowdStrike	ThreatConnect	ip_address		Success	deploy_admin
06/27/2024 05:32:42 am	Contain host on CrowdStrike	ThreatConnect	ip_address		Success	deploy_admin
06/27/2024 05:31:22 am	Contain host on CrowdStrike	ThreatConnect	ip_address		Failed	deploy_admin
06/27/2024 05:30:43 am	Contain host on CrowdStrike	ThreatConnect	ip_address		Failed	deploy_admin

To view Action History

1. Go to  (CONFIGURE) > **More** > **Response Actions**.

The **Response Actions** view is displayed.

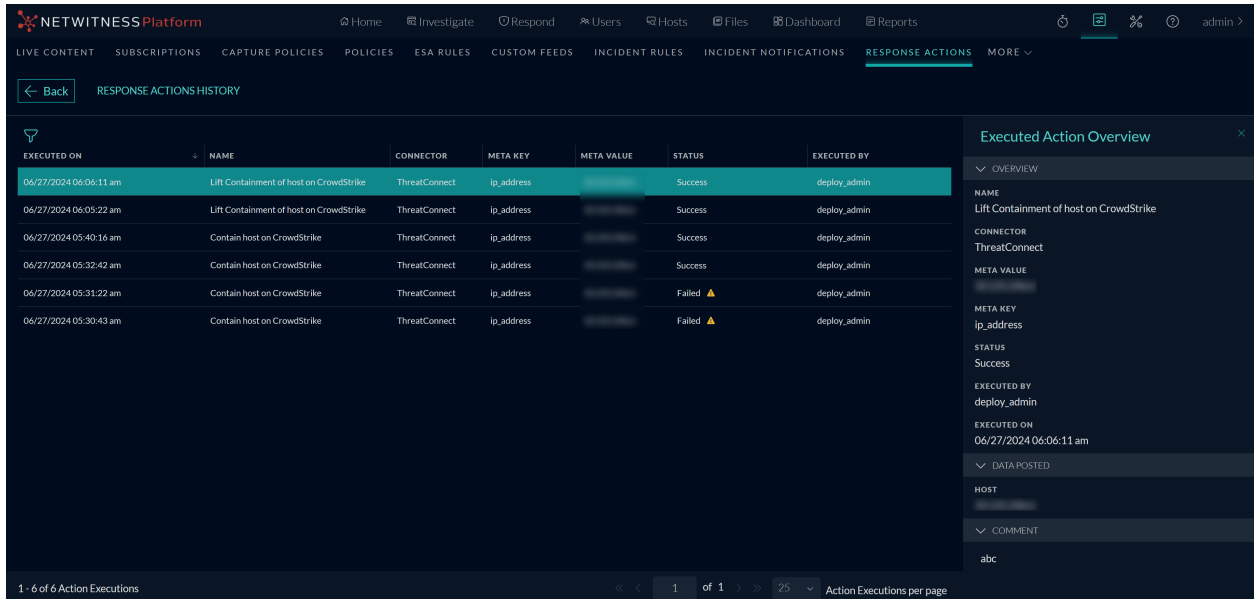
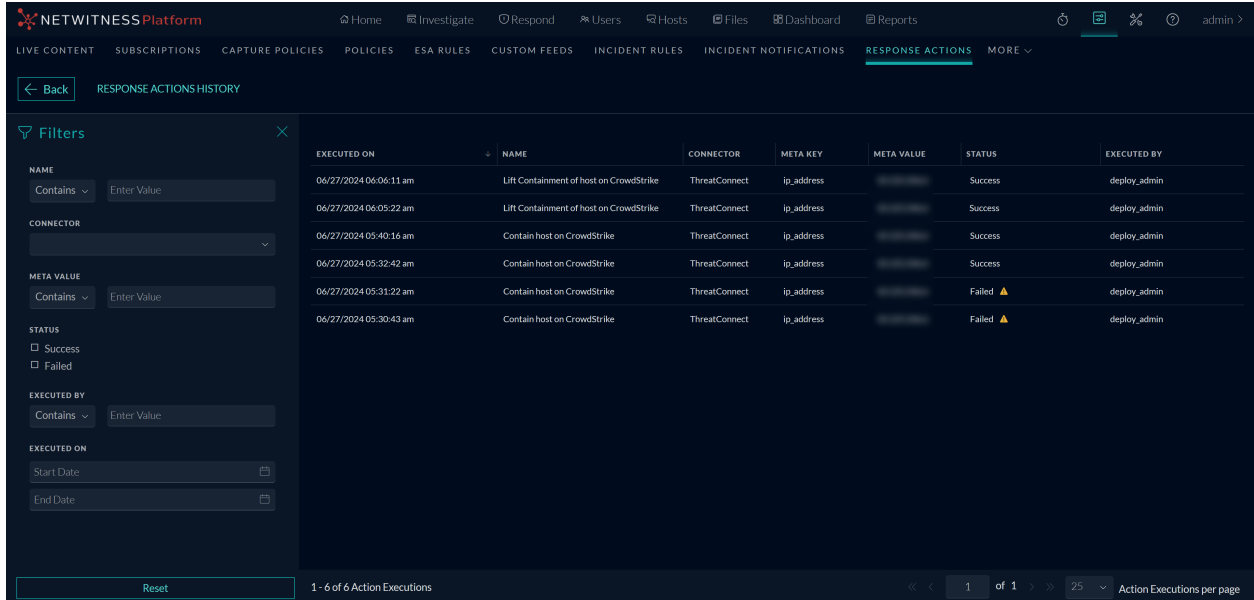
NAME	DESCRIPTION	CONNECTOR	META KEYS	STATUS	LAST UPDATED
Contain host	This response action contains an host via crowdstrike whic...	CrowdStrike	alias.ip, device.ip, forward.ip (26)	Enabled	06/19/2024 06:
Contain host on CrowdStrike	This response action contains an host using NetWitness Pr...	ThreatConnect	alias.ip, device.ip, forward.ip (25)	Enabled	06/27/2024 09:
Lift Containment of host on CrowdStrike	This response action lifts containment on a host using Net...	ThreatConnect	alias.ip, device.ip, forward.ip (25)	Enabled	06/27/2024 06:
Lift Containment on host	This response action lifts containment on a host via crowdst...	CrowdStrike	alias.ip, device.ip, forward.ip (25)	Enabled	06/19/2024 06:

2. Click **View Action History**.

The **Response Actions History** view is displayed.

Response Actions History View

The Response Actions History view consists of a Filters panel, Response Actions History List, and an Overview panel.



Response Actions History Filters Panel

You can apply the following filters to view the history of the Response Actions of your interest.

- Response Actions Name
- Meta Value
- Response Actions execution Status
- User who executed the Response Action
- Time duration between which the Response Action was executed

The following table lists all the fields displayed in the Response Actions History Filters Panel.

Fields	Description
Name	Allows you to enter the name of the required Response Action.
Meta Value	Allows you to enter the value of the meta key associated with the Response Action.
Status	Allows you to filter the Response Action on the basis of the execution status. For example: If you could successfully send the meta and other parameters to the connector after executing the Response Action, you can select Success status to filter the required ResponseAction and vice-versa.
Executed By	Allows you to filter the Response Action on the basis of the user who executed the Response Action.
Executed On	Allows you to select the time duration between which the Response Action was executed.

Response Actions History List

The Response Actions History List displays the history of all the Response Actions executed in the NetWitness Platform.

The following table describes the columns in the Response Actions History List.

Columns	Description
Executed On	Displays the date and time when the Response Action was last executed. For example: 12/11/2023 05:06am
Name	Displays the name of all the Response Actions executed.
Connector	Displays the name of the third party tool for which the particular Response Action was executed. For example: ThreatConnect
Meta Key	Displays the list of meta keys for which the Response Action was executed. For example: ip.src
Meta Value	Displays the value of the meta key for which the Response Action was executed. For example: 10.125.237.89
Status	Displays the status of the execution of Response Action. For example: Success and Failed .

Columns	Description
Executed By	Displays the name of the user who executed the Response Action last time.

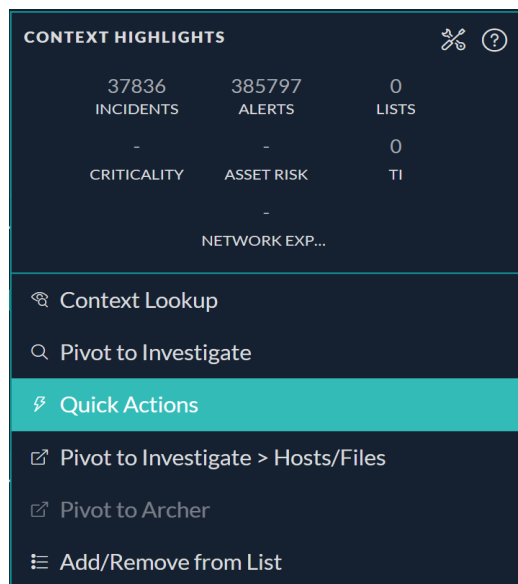
Response Actions History Overview panel

When you click any row in the Response Actions History List, the Overview panel is displayed on the right side of the Response Actions History view which shows the basic summary information about the particular Response Action executed. The following fields and parameters are displayed in the Overview panel.

- Name:** This field displays the name of the Response Action executed.
 For example: If you provided **Block IP** as the Response Action name while executing the Response Action, the same **Block IP** name will be displayed in the **Name** field in the Response Actions History Overview panel.
- Connector:** This field displays the connector name associated with the Response Action executed.
 For example: ThreatConnect.
- Meta Value:** This field displays the meta value associated with the Meta Key.
 For example: If the supported Meta Key is **ip.src**, the meta value will be displayed in the form of an IP address such as **10.125.246.29**.
- Meta Key:** This field displays the supported Meta Key for which the particular Response Action was executed.
 For example: **ip.src** and **mac_address**.
- Status:** This field displays the status of the Response Action executed.
 For example: If the meta key and the additional parameters are forwarded to the connector successfully, the **Status** field displays **Success**. If the meta key and the additional parameters are not forwarded to the connector after performing the Quick Action, the **Status** field displays **Failed**.
- Executed By:** This field displays the name of the user who executed the Response Action last time.
- Executed On:** This field displays the Date and Time when the Response Action was last executed
 For example: **12/19/2023 07:32:01 am**
- Additional Parameters such as Parameter Key and Parameter Label that are posted to the connector.
 For example: The **Data Posted** section in the Response Actions History Overview panel displays the meta keys and additional parameters posted to the connector.
- Comment provided during the execution of the Response Action.
 For example: **Post the parameters and the meta key to ThreatConnect.**

Quick Actions

The **Quick Actions** option introduced in the **Context Highlights** section allows users to use the response action configured for any applicable meta and send the meta along with any additional parameters to the third party tool for further processing.



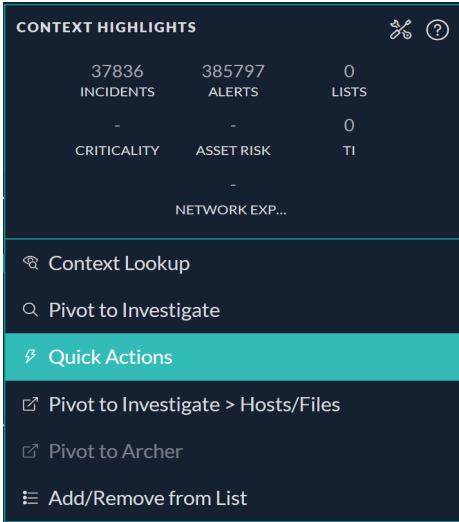
Note: You can access **Quick Actions** option when you right click any context meta in **Investigate**, **Respond**, **Users**, and **Hosts** view where Context Highlights appears. By default, the **Quick Actions** option is enabled in **Context Menu Action Configuration** dialog (Admin > System > Context Menu Actions > Quick Actions > Context Menu Action Configuration).

Execute Quick Actions Option

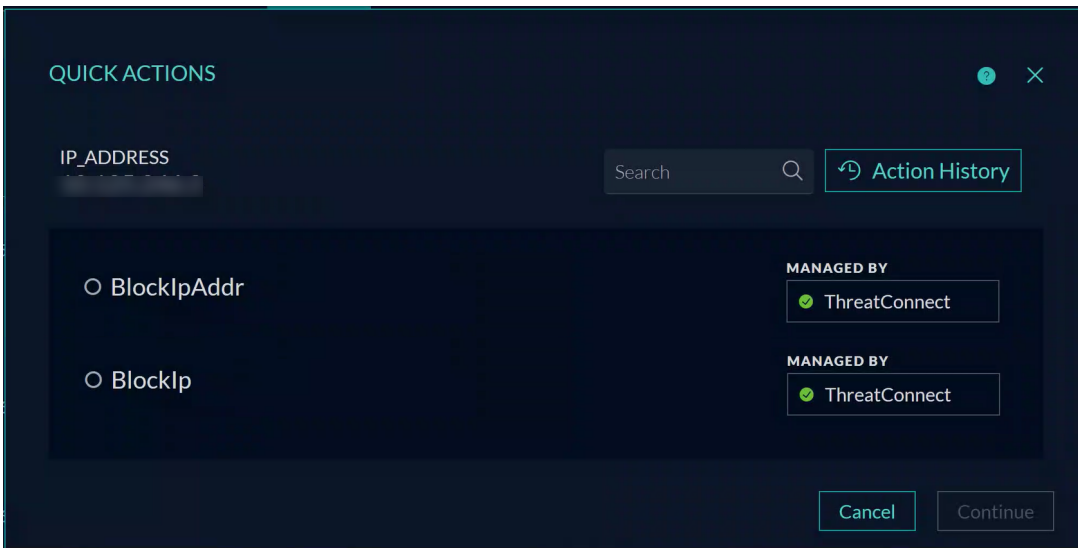
You can take a quick action on any applicable meta in **Respond**, **Users**, **Investigate**, and **Hosts** view.

To take a Quick Action on the applicable meta

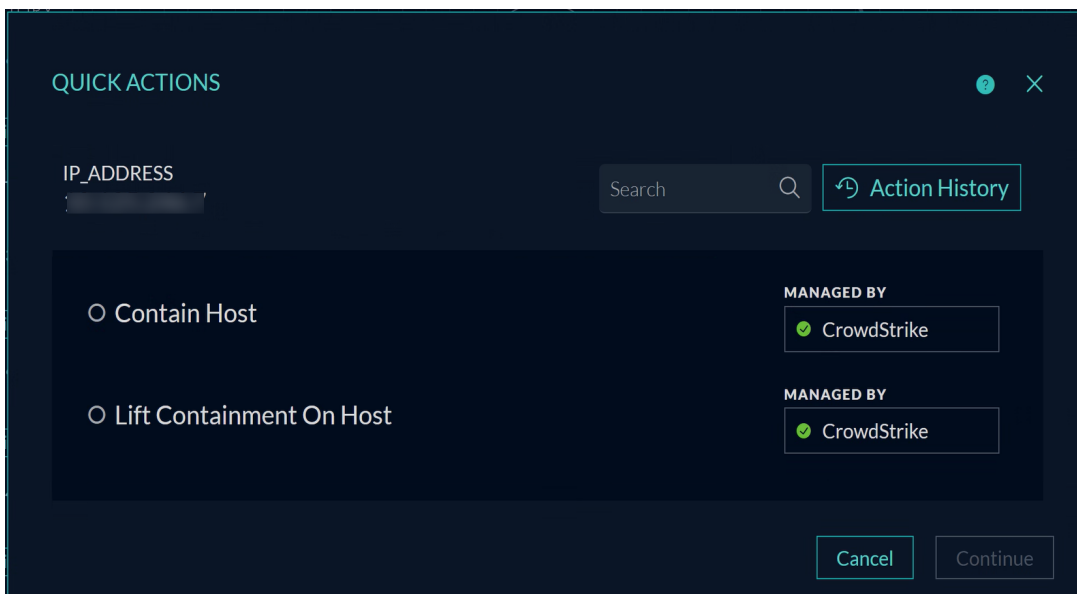
1. (Optional) Create Response Action for the applicable meta in the **Create Response Action** view.
2. Right click the meta in **Respond**, **Users**, **Investigate**, or **Hosts** view.
The **Context Highlights** section is displayed.



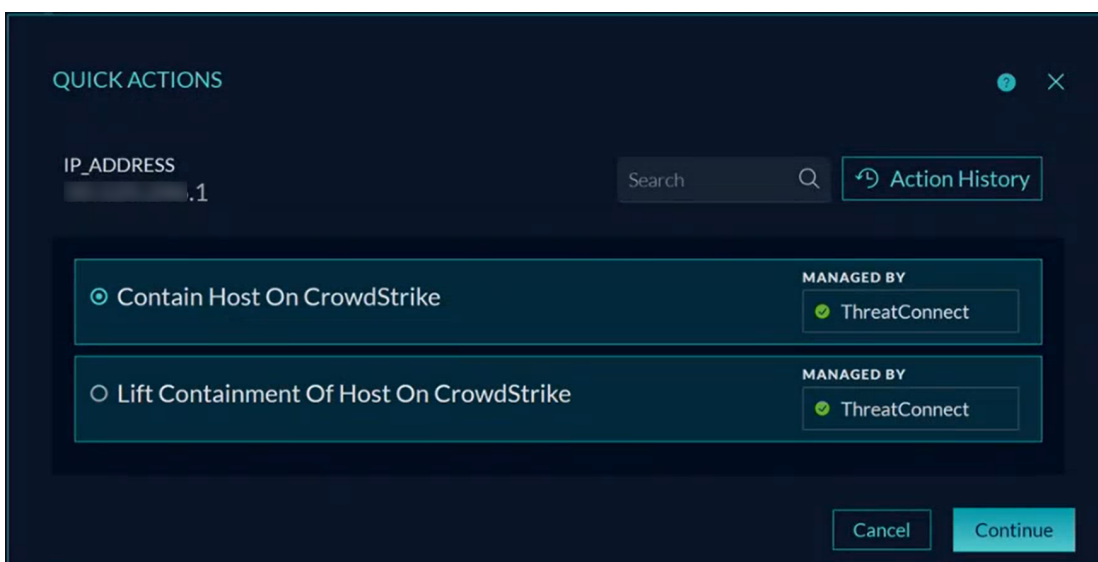
3. Select the **Quick Actions** option.
The **Quick Actions** window is displayed.
Quick Actions for ThreatConnect:



Quick Actions for CrowdStrike:



Quick Actions for CrowdStrike through ThreatConnect:



4. Select the required Response Action and click **Continue**.
5. Enter the additional parameters information, if any.

Note: This is applicable only if you have created custom Response Actions for ThreatConnect.

Note: For more information on how to add the additional parameters information in the **Quick Actions** window, see [Response Actions and Quick Actions Use Case Examples](#).

6. Enter the comments and click **Confirm**.

Response Actions and Quick Actions Use Case

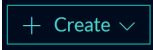
Examples

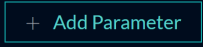
The following use cases provide examples of an administrator and an analyst using NetWitness Platform to manage Response actions and send the additional parameters along with the meta to ThreatConnect connector for further processing.

Use Case #1: Managing Response Action and taking Quick Action in Respond view for the supported meta

Note: This Use Case is only for Custom Response Actions for ThreatConnect.

After integrating the third-party tool ThreatConnect with NetWitness Platform, administrator John navigates to the **Response Actions** view ( (CONFIGURE) > **More** > **Response Actions**) and performs the following actions.

- Creates new Response Action: Administrator John clicks the  option in the Response Actions toolbar and enters the following details in the **Create Response Action** view.
 - Response Action Name
 - Description of the Response Action
 - Metas supported for Response Action
 - URL path associated with the connector

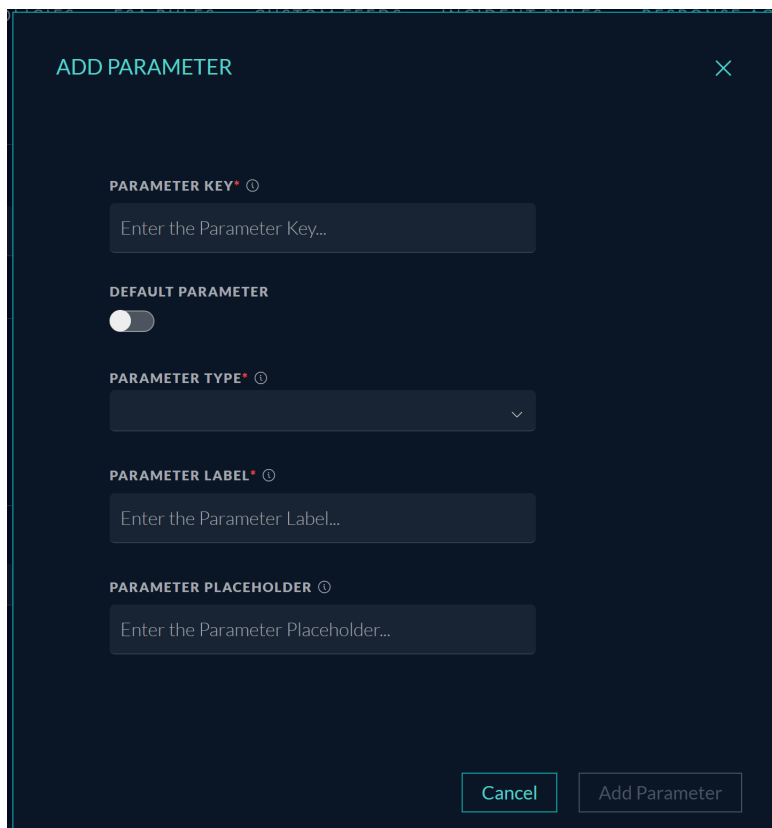
Finally, the administrator clicks  besides the **Parameters** field and creates the default parameter in the **Add Parameter** window. This is used as the key in the key-value pair associated with the value of the meta selected that is sent to ThreatConnect.

- Parameter Key: Administrator John enters **ip-meta** in this field.
- Default Parameter: Enabled

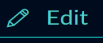
After entering these details, John clicks **Add**. Now, the admin clicks  besides the **Parameters** field and creates an additional parameter he would like to send to ThreatConnect.

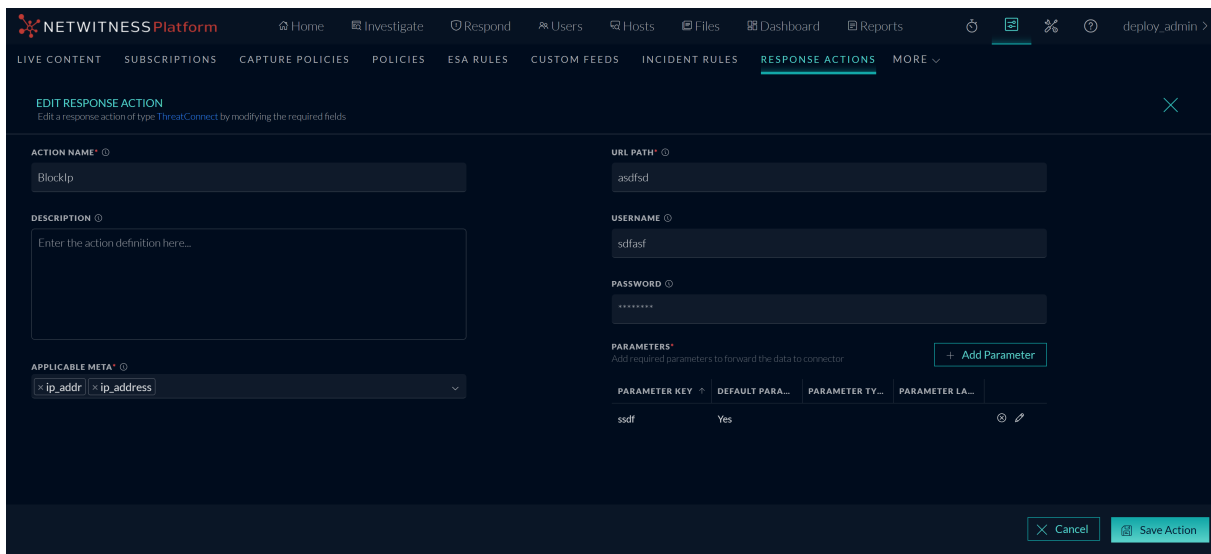
- Parameter Key: Administrator John enters **additional-ip** in this field.
- Parameter Type: Administrator John selects **IP** in this field.
- Parameter Label: Administrator John enters **Additional IP Address to Block** in this field.
- Parameter Placeholder: Administrator John enters **Additional IPs** as the placeholder text in this field.

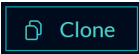
After entering these details, John clicks **Add Parameter**.

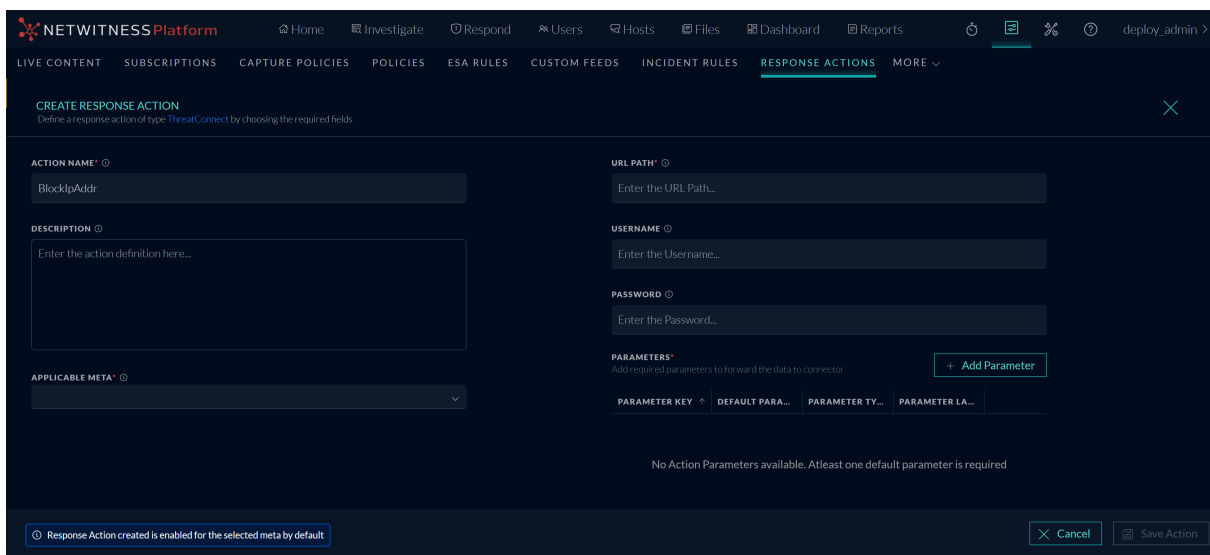



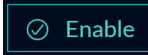

As the last step, John clicks **Save Action**.

- Edits the Response Action: John selects the newly created Response Action and clicks the  **Edit** option in the Response Actions toolbar. As soon as the **Edit Response Action** view is displayed, the admin adds a new meta ip.src to the existing list of the Applicable metas in **Applicable Meta** field and clicks **Save Action**.

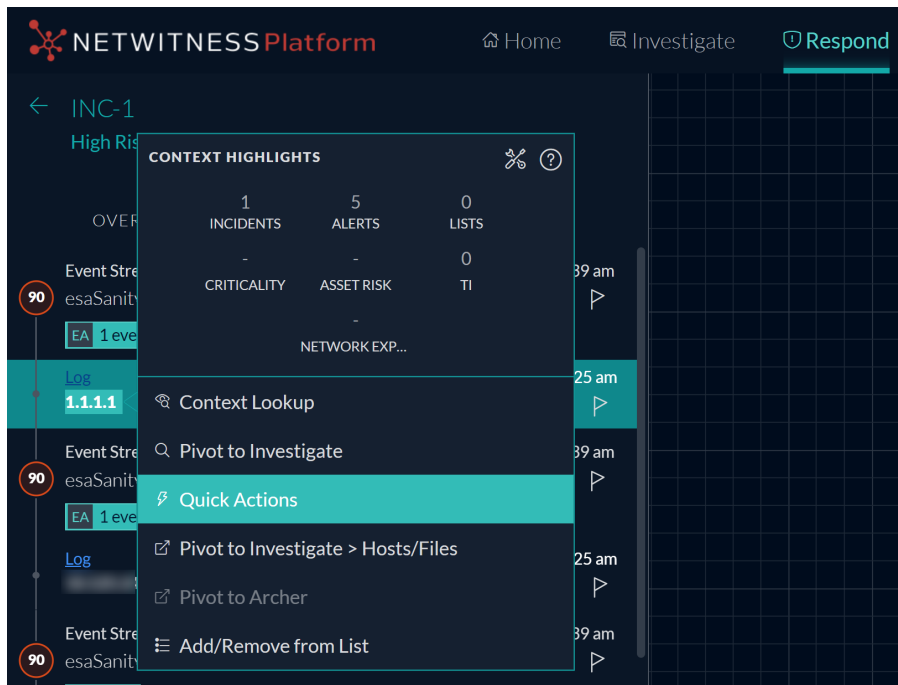


- Clones the Response Action: After editing the Response Action, the admin selects an existing Response Action and clicks the  **Clone** toolbar option in the Response Actions toolbar. Once the **Create Response Action** view is displayed, admin John modifies the Action Name **Block IP** to **Block IP Addr** and clicks **Save Action**.

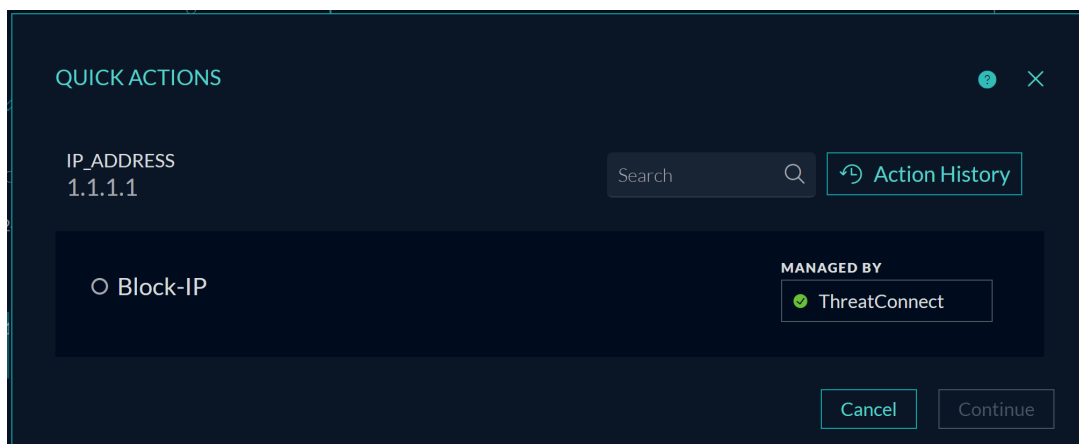


- Disables the Response Action: Administrator John decides to disable the Response Action in the **Response Actions** view. Therefore, to disable the Response Action, John selects the Response Action and clicks the  **Disable** option in the Response Actions toolbar.
- Enables the Response Action: Administrator John decides to re-enable the Response Action in the **Response Actions** view. Therefore, to re-enable the Response Action, John selects the Response Action and clicks the  **Enable** option in the Response Actions toolbar.
- Deletes the Response Action: John creates a new Response Action and decides to delete the previous Response Action he created. To delete the Response Action, John selects that Response Action and clicks the  **Delete** option in the Response Actions toolbar.

After performing the above actions, administrator John navigates to the **Respond > Alerts** view. The administrator clicks the Alert name in the **Name** column in the Alerts List view and then right clicks the Source IP value (supported meta) **1.1.1.1** once the **Event Details** view is displayed. When the **ContextHighlights** section is displayed, John selects the **Quick Actions** option.



As soon as the **Quick Actions** window is displayed, John selects the Response Action he created for the meta and clicks **Continue**.



In the next step, he observes that the parameter label he entered while adding parameters is now appearing as a field in the **Quick Actions** window.

The screenshot shows a dark-themed dialog box titled "QUICK ACTIONS" with a close button (X) in the top right corner. The main content area is divided into several sections:

- Block-IP** (with an information icon) and the IP address **1.1.1.1**.
- MANAGED BY**: A box containing a green checkmark and the text "ThreatConnect".
- ADDITIONAL IP ADDRESS TO BLOCK**: A text input field with the placeholder text "Additional IPs, Use commas to separate multiple values."
- COMMENTS**: A larger text input field with the placeholder text "Enter Comments".

At the bottom right of the dialog, there are three buttons: "Cancel", "Back", and "Confirm".

Then, John enters **1.1.1.0/24** in the **Additional IP Address to Block** field (parameter label added), enters the comment as **These are unrecognized hosts** and finally clicks **Confirm**.

After executing the Response Action, the following JSON is posted to ThreatConnect.

```
{
  "ip-meta": "1.1.1.1",
  "additional-ip" : ["1.1.1.0/24"]
  "nw-user" : "tony",
  "nw-comment" : "These are unrecognized hosts",
  "nw-actionId" : "8635834894350nbd99025356",
  "nw-actionName": "Block-IP"
}
```

Here,

"ip-meta": "1.1.1.1" is the supported meta for which the Response Action is executed.

"additional-ip" : ["1.1.1.0/24"] is the parameter label value posted to ThreatConnect.

"nw-user" : "tony" is the user who executed the Response Action.

"nw-comment" : "These are unrecognized hosts" is the comment provided while executing the Response Action.

"nw-actionId" : "8635834894350nbd99025356" is the ID associated with this specific Response Action executed.

"nw-actionName": "Block-IP" is the name of the Response Action executed.

Use Case #2: Taking Quick Action in Investigate view for the supported meta

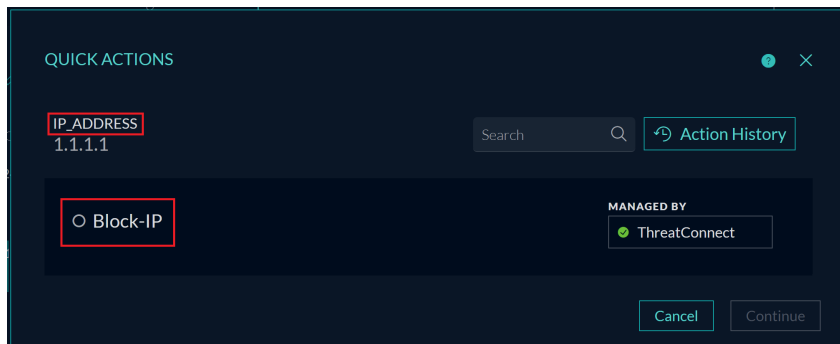
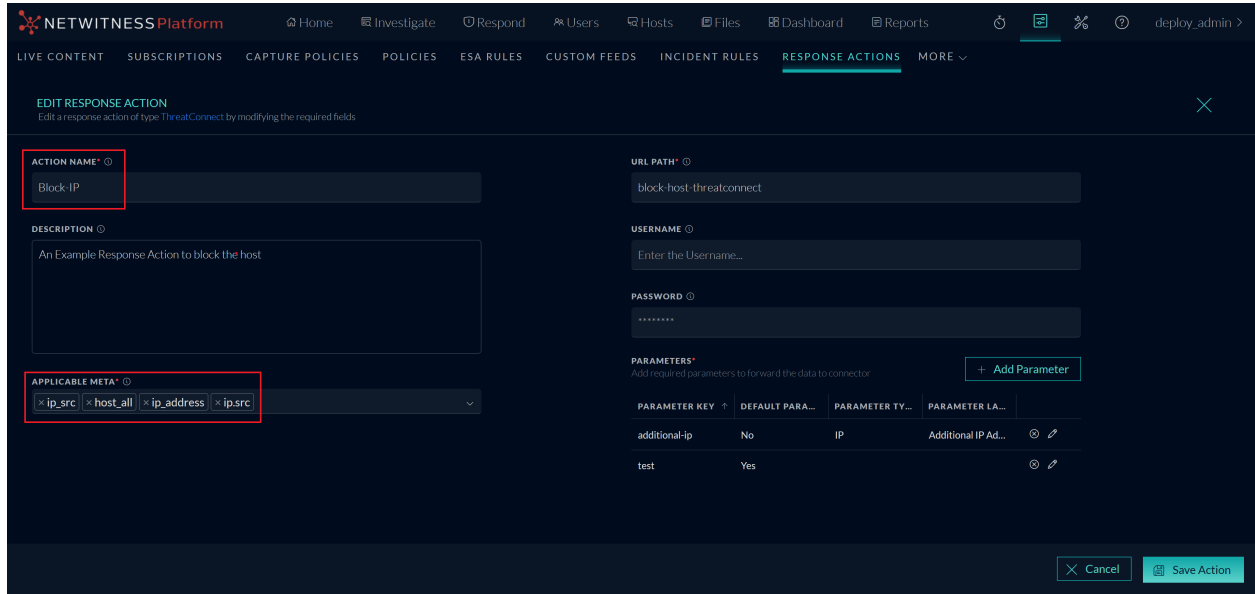
Kevin, an analyst, navigates to the **Investigate > Events** view and queries the events. Kevin finds the meta key **ip.src** with value **10.12.12.12** in the **Summary** column in the **Events** view and decides to take a Quick Action on the meta. As the first step, Kevin creates the Response Action for the meta using the **Response Actions** view. After creating the Response Action, Kevin navigates back to the **Investigate > Events** view and right clicks the meta to select the **Quick Actions** option under the **Context Highlights** section. After clicking the **Quick Actions** option, Kevin selects the newly created Response Action in the **Quick Actions** window and clicks **Continue**. In the next step, Kevin enters the value for the Additional Parameter configured while creating the Response Action. Finally, Kevin enters the comment and clicks **Confirm**.

Use Case #3: Taking Quick Action in Investigate view for the supported meta for OOTB Response Actions

Kevin, an analyst, navigates to the **Investigate > Events** view and queries the events. Kevin finds the meta key **ip.src** with value **10.12.12.12** in the **Summary** column in the **Events** view and decides to take a Quick Action on the meta. As the first step, Kevin ensures connector is configured and performs the OOTB action. Kevin navigates back to the **Investigate > Events** view and right clicks the meta to select the **Quick Actions** option under the **Context Highlights** section. After clicking the **Quick Actions** option, Kevin selects the required action in the **Quick Actions** window and clicks **Continue**. Finally, Kevin enters the comment and clicks **Confirm**.

Correlation between Response and Quick Actions

In the **Use Case #1: Managing Response Action and taking Quick Action for the supported meta in Respond view** above, you can observe that the fields or options appearing in the **Quick Actions** window are the values entered while configuring the Response Action. For example, refer the following figures.



In the above example, if you observe, the Action Name **Block-IP** entered while configuring the Response Action is now appearing as an option below the supported meta key with value **1.1.1.1** in the **Quick Actions** window.

Similarly, the value of the Parameter Label entered in the **Add Parameter** window while configuring the Response Action, appears as the field below the Response Action name in the **Quick Actions** window, and the Parameter Placeholder value entered in the **Add Parameter** window while configuring the Response Action, appears as the placeholder text under the Parameter Label value field in the **Quick Actions** window. Refer the following figures.

ADD PARAMETER ✕

PARAMETER KEY* ⓘ
additional-ip

DEFAULT PARAMETER

PARAMETER TYPE* ⓘ
IP

PARAMETER LABEL* ⓘ
Additional IP Address to Block

PARAMETER PLACEHOLDER ⓘ
Additional IPs

Cancel Add Parameter

QUICK ACTIONS ⓘ ✕

Block-IP ⓘ
1.1.1.1

MANAGED BY
✔ ThreatConnect

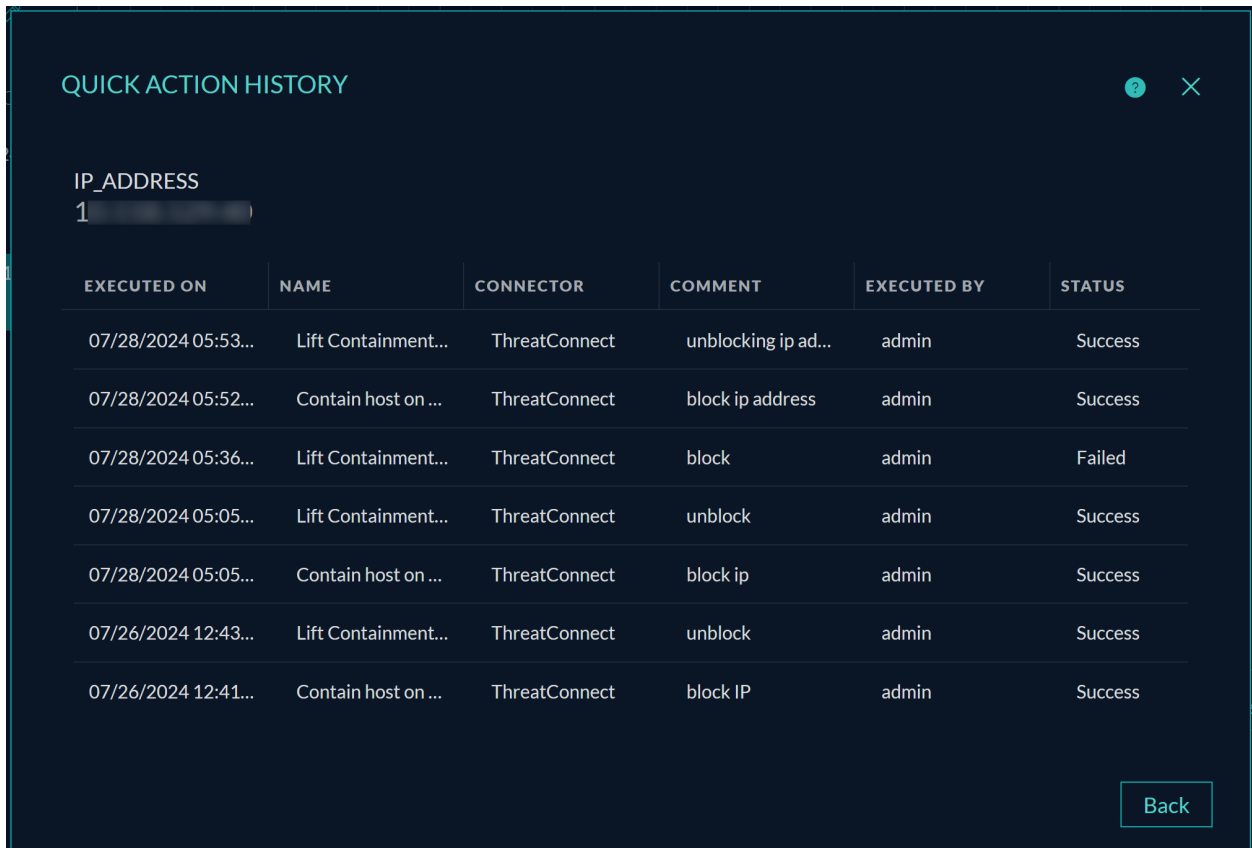
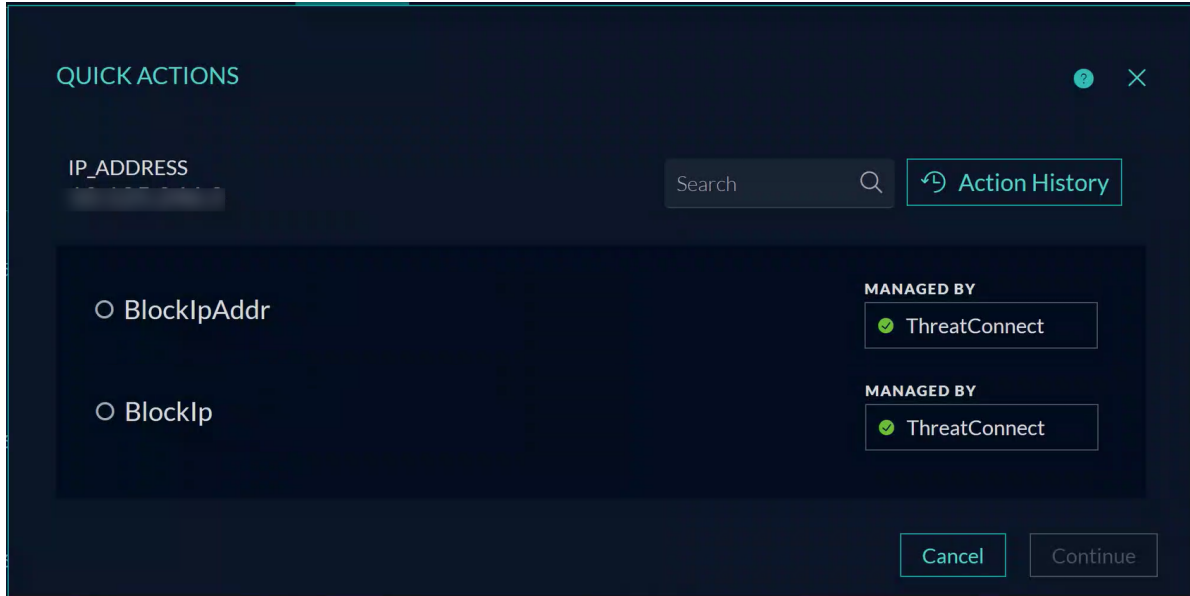
ADDITIONAL IP ADDRESS TO BLOCK
Additional IPs, Use commas to separate multiple values.

COMMENTS *
Enter Comments

Cancel Back Confirm

Quick Action History


When you click the **Action History** option in the **Quick Actions** window, the **Quick Action History** window displays the historical details of the Response Actions executed for that specific meta value.



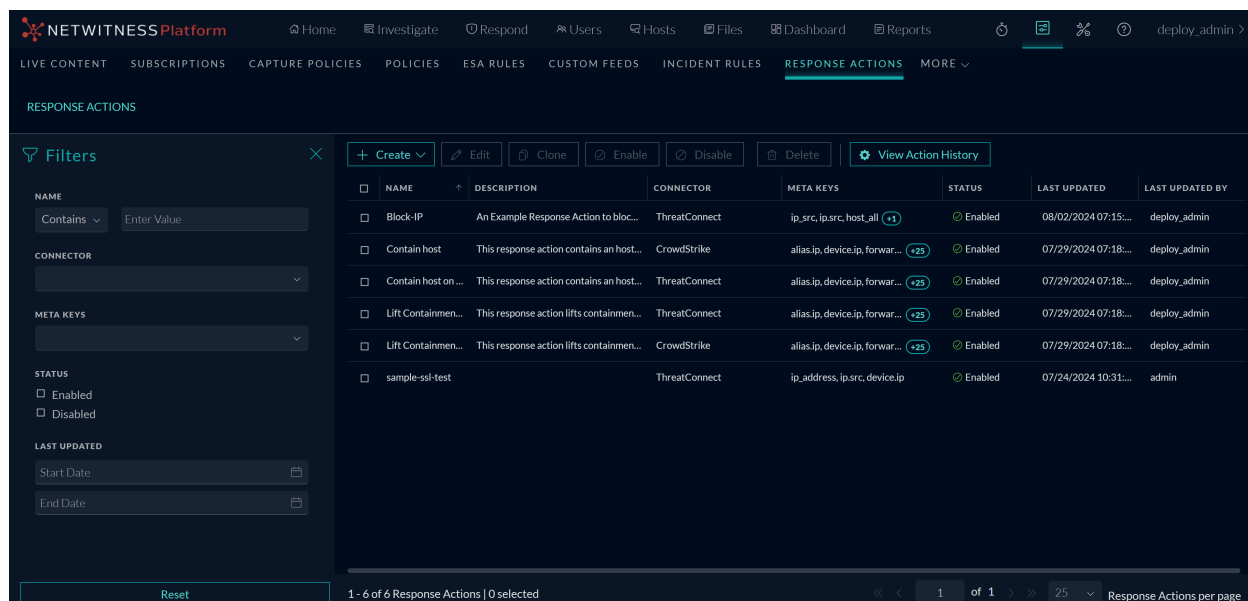
The following table describes the columns in the **Quick Action History** view.

Columns	Description
Executed On	Displays the date and time when the Response Action was last executed. For example: 12/11/2023 05:06am
Name	Displays the name of all the Response Actions executed.
Connector	Displays the name of the third party tool for which the particular Response Action was executed. For example: ThreatConnect or CrowdStrike
Comment	Displays the comment provided while executing the Response Action.
Executed By	Displays the name of the user who executed the Response Action last time.
Status	Displays the status of the execution of Response Action. For example: Success and Failed .

Response Actions List view

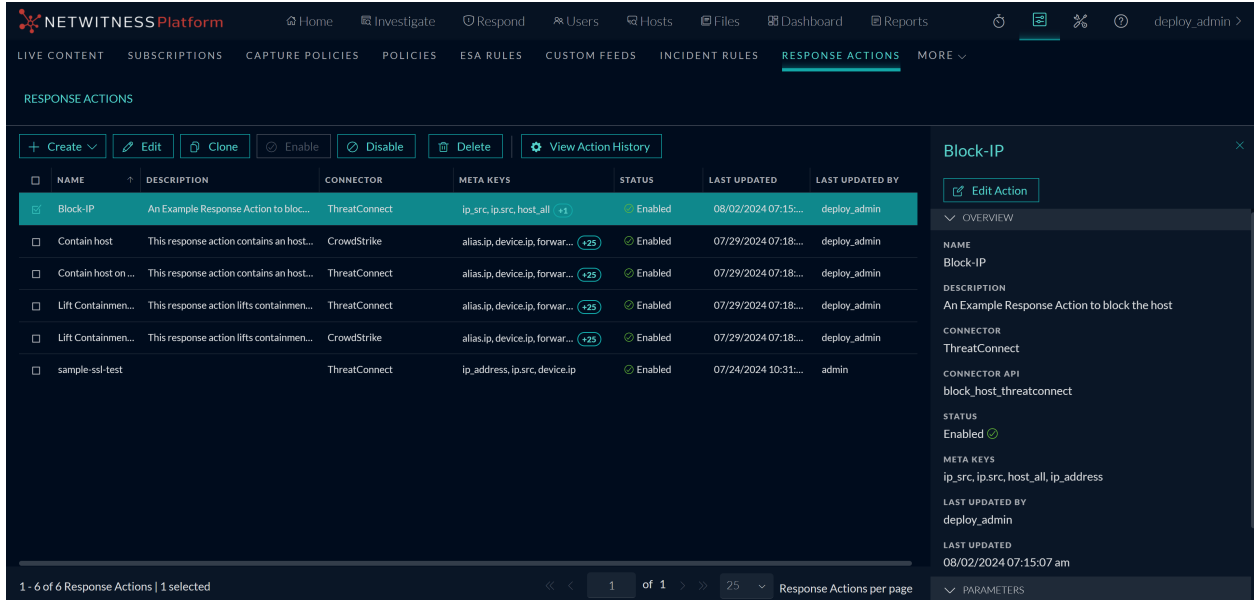
The Response Actions List view ( (CONFIGURE) > More > Response Actions) allows you to manage the Response Actions configured. The Response Actions List View consists of the Filters Panel, Response Actions List, and an Overview panel.

The following figure shows the Filters Panel on the left and the Response Actions List on the right.



NAME	DESCRIPTION	CONNECTOR	META KEYS	STATUS	LAST UPDATED	LAST UPDATED BY
Block-IP	An Example Response Action to bloc...	ThreatConnect	ip_src,ip_src_host_all	Enabled	08/02/2024 07:15...	deploy_admin
Contain host	This response action contains an host...	CrowdStrike	alias.ip,device.ip,forwar...	Enabled	07/29/2024 07:18...	deploy_admin
Contain host on ...	This response action contains an host...	ThreatConnect	alias.ip,device.ip,forwar...	Enabled	07/29/2024 07:18...	deploy_admin
Lift Containmen...	This response action lifts containmen...	ThreatConnect	alias.ip,device.ip,forwar...	Enabled	07/29/2024 07:18...	deploy_admin
Lift Containmen...	This response action lifts containmen...	CrowdStrike	alias.ip,device.ip,forwar...	Enabled	07/29/2024 07:18...	deploy_admin
sample-ssl-test		ThreatConnect	ip_address,ip_src,device.jp	Enabled	07/24/2024 10:31...	admin

The following figure shows the Response Actions Overview panel on the right.



Response Actions List

The Response Actions List displays all the Response Actions configured in the NetWitness Platform. You can filter this list to view only the Response Actions of interest.

The following table describes the columns in the Response Actions List.

Columns	Description
Name	Displays the name of all the Response Actions in the Response Actions List view.
Description	Displays the descriptions of the Response Actions.
Connector	Displays the name of the third party tool for which the particular Response Action is configured.
Meta Keys	Displays the list of meta keys for which the Response Action is supported.
Status	Displays the current status of the Response Action. For example: Enabled and Disabled .
Last Updated	Displays the date and time when the Response Action was last updated.
Last Updated By	Displays the name of the user who updated the Response Action last time.

Response Actions Filters Panel

You can filter the Response Actions based on the following parameters.

- Response Action Name
- Status of the Response Action

- Supported Meta Keys
- Last updated Date and Time

The following table lists all the fields displayed in the Response Actions Filters panel.

Fields	Description
Name	Allows you to enter the name of the required Response Action.
Status	Allows you to filter the Response Action on the basis of the status. For example: You can select Enabled or Disabled status to filter the required Response Action.
Connector	Allows you to select the third party tool for which the particular Response Action was executed. For example: ThreatConnect or CrowdStrike
Meta Keys	Allows you to filter the Response Action on the basis of the meta keys supported.
Last Updated	Allows you to filter the Response Action on the basis of the date and time when the action was last updated.



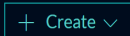
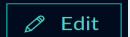
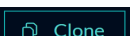
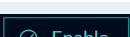

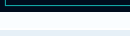
Response Actions Overview panel

When you click any row in the Response Actions List, the Overview panel is displayed on the right side of the Response Actions List view which shows the basic summary information about the particular Response Action. The following fields and parameters are displayed in the Overview panel.

- Name of the Response Action
- Description of the Response Action
- Connector Name
- Connector API
- Status of the Response Action
- Supported Meta Keys
- Name of the user who updated the Response Action last time
- Date and Time when the Response Action was last updated
- IP – Meta
- Additional Parameters

Toolbar Actions in Response Actions view

The table below lists the toolbar actions available in the Response Actions view.

Option	Description
	Select this option to view the required Response Actions in the Response Actions List view.
	Select this option to delete the required Response Action.
	Select this option to create a new Response Action. This option is grayed out if you have not integrated any connector with NetWitness platform. If the connector is integrated with NetWitness Platform, you can select the same from the drop-down list.
	Select this option to edit the existing Response Action.
	Select this option to clone the existing Response Action.
	Select this option to enable an already disabled Response Action.
	Select this option to disable the selected Response Action.
	Select this option to view the history of the Response Actions.

Connect with Threat Connect using HTTPS

The SSL connection between ThreatConnect and NetWitness Platform ensures that the data forwarded to the ThreatConnect instance through NetWitness Platform is completely secure.

You can establish the HTTPS connection between the ThreatConnect instance and NetWitness Platform with or without SSL certificate verification depending on whether the `verify-s-s-l` is marked as true or false.

Establish HTTPS connection with SSL certificate verification

You must export the SSL certificate from ThreatConnect instance and add the certificate to the Response Actions service trust-store for SSL certificate verification.

To perform SSL certificate verification using ThreatConnect Instance

1. Obtain the SSL certificate from ThreatConnect instance.

Note: Depending upon the implementation of ThreatConnect Playbook, you can obtain the certificate through different modes.

For example: If the ThreatConnect Playbook is implemented as Webhook Trigger, the certificate viewer associated with the browser can be used to export the certificate. The certificate exported is as shown in the following figure.

Certificate

threatconnect	
Subject Name	
Common Name	threatconnect
Issuer Name	
Common Name	threatconnect
Validity	
Not Before	Sun, 10 Aug 2014 09:30:45 GMT
Not After	Wed, 07 Aug 2024 09:30:45 GMT
Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	81:F0:87:C7:BF:9C:58:49:3F:24:C0:73:43:7E:6D:86:EE:73:6D:97:4A:B6:DB:9A:8B:3D:...
Miscellaneous	
Serial Number	53:E7:3B:C5
Signature Algorithm	SHA-1 with RSA Encryption
Version	1
Download	PEM (.cert) PEM (.chain)

2. Ensure that the certificate obtained is in **.pem** format. If the certificate obtained is not in **.pem** format, you must convert the format to **.pem**.

Note: If multiple intermediate Certificate Authorities (CAs) are present in the connection between NetWitness Platform and ThreatConnect, all the certificates of the certificate chain must be uploaded to service trust-store in **.pem** format. If the certificates are transferred between the Operating Systems such as Windows and Linux, the format of the certificates must be adjusted.

3. Place the certificate on Admin-Server and run the following command.



```
security-cli-client --add-trusts -s response-actions-server -x /root/threatconnect-chain.pem -u deploy_admin -k <deploy_admin_password>
```

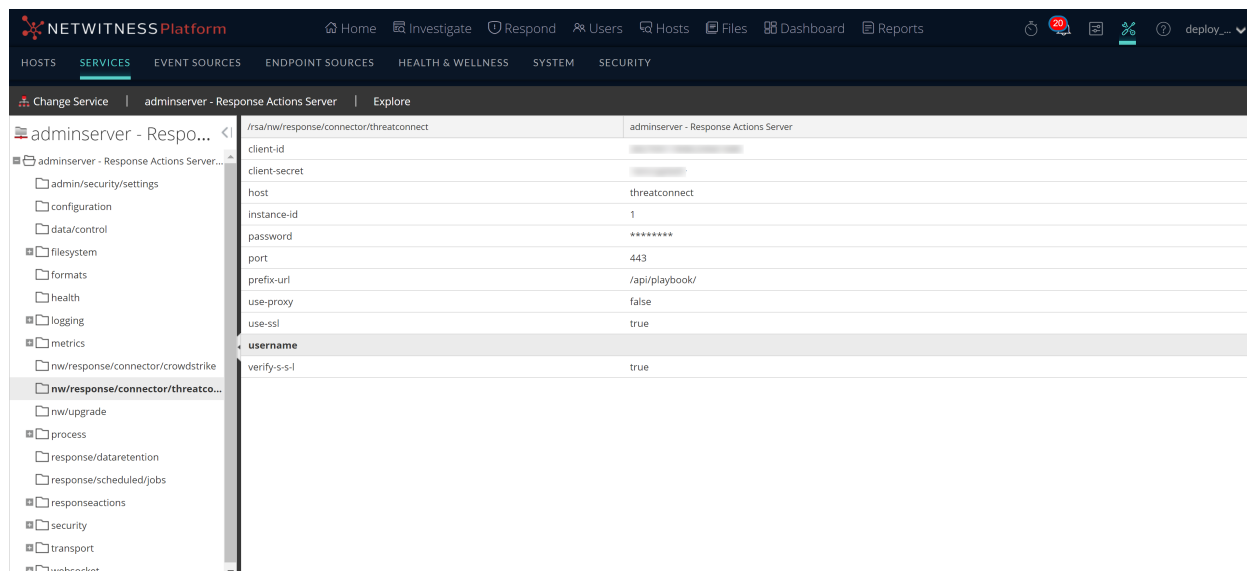
4. Capture the CommonName (CN) from the certificate and add it as the host mapping under `/etc/hosts` file.

For example: If **threatconnect** is the CommonName captured from the certificate, you must append the following entry to the `/etc/hosts` file.

#threatconnect-instance-ip CommonName-present-in-certificate

1.1.1.x threatconnect .

5. Go to  (Admin) > Services > select the Response Actions Server service >  > **View > Explore > nw/response/connector/threatconnect.**
6. Enter the CommonName (CN) captured (in **Step-4**) in the **host** field.
7. Enter **true** in the **use-ssl** field.
8. Enter **true** in the **verify-s-s-l** field.
9. In the **port** field, enter the appropriate port on which the ThreatConnect instance is connected. By default, the SSL port is **443**.





The screenshot shows the NetWitness Platform interface. The top navigation bar includes Home, Investigate, Respond, Users, Hosts, Files, Dashboard, and Reports. The main content area is titled 'adminserver - Response Actions Server' and shows a configuration table for the 'nw/response/connector/threatconnect' connector.



Field	Value
client-id	[REDACTED]
client-secret	[REDACTED]
host	threatconnect
instance-id	1
password	*****
port	443
prefix-url	/api/playbook/
use-proxy	false
use-ssl	true
username	[REDACTED]
verify-s-s-l	true

Establish HTTPS connection without SSL certificate verification

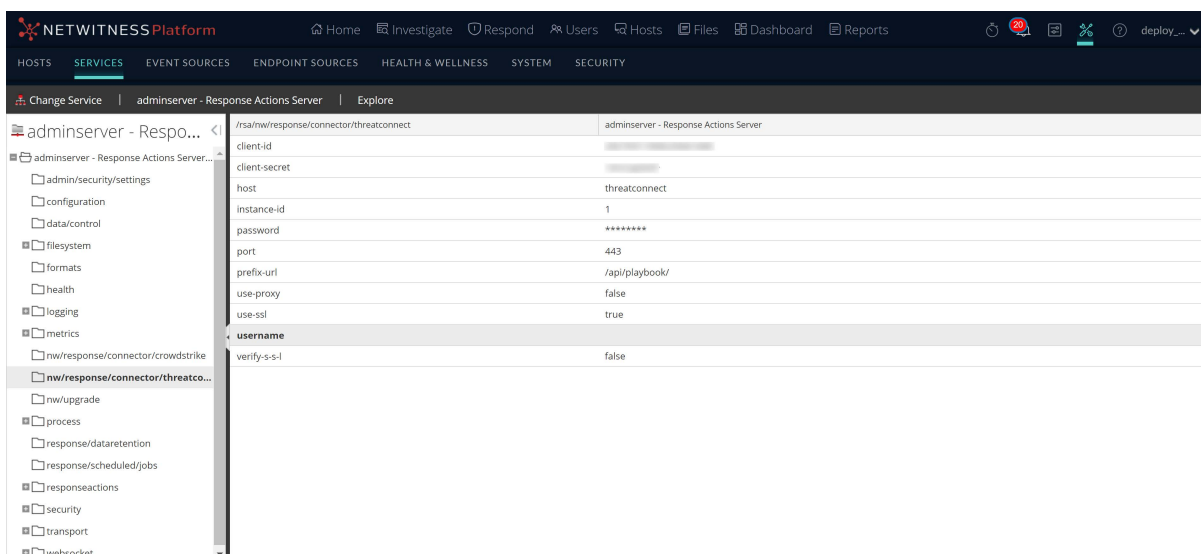
You can establish the SSL connection between ThreatConnect and NetWitness Platform without SSL certificate verification.

To skip SSL certificate verification

1. Go to  (Admin) > **Services** > select the Response Actions Server service >  > **View** > **Explore** > `nw/response/connector/threatconnect`.
2. Enter **true** in the **use-ssl** field.
3. Enter **false** in the **verify-s-s-l** field.

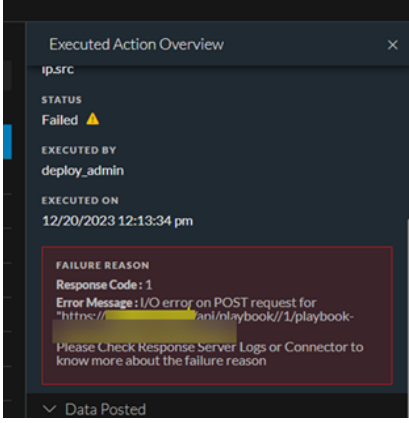
Note: When **verify-s-s-l** field is set to **false**, you can enter the IP address or DNS mapping of ThreatConnect Instance in the **host** field in  (Admin) > **Services** > select the Response Actions Server service >  > **View** > **Explore** > `nw/response/connector/threatconnect`.

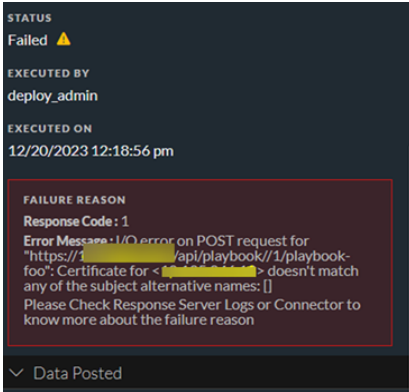


4. In the **port** field, enter the appropriate port on which the ThreatConnect instance is connected. By default, the SSL port is **443**.






Troubleshooting

This section lists the troubleshooting information for the various issues encountered while integrating and executing Response Actions.

<p>Error</p>	
<p>Problem</p>	<p>The Response Action execution fails if you do not upload the SSL certificate to the Response Actions Server service trust-store after setting the verify-s-s-l configuration to true in the Response Actions Server Explore view. Consequently, the above error is displayed in the Response Actions History Overview panel.</p>
<p>Workaround</p>	<p>You must upload the SSL certificate to the Response Actions Server service trust-store after setting the verify-s-s-l configuration to true in the Response Actions Server Explore view.</p>

<p>Error</p>	
<p>Problem</p>	<p>The Response Action execution fails if you do not perform the following actions after adding the SSL certificate to the Response Actions Server service trust-store.</p> <ul style="list-style-type: none"> - Adding the CommonName (CN) of the certificate as the host mapping in <code>/etc/hosts</code> file. - Entering the CommonName (CN) of the certificate in the host field in  <p>(Admin) > Services > select the Response Actions Server service >  > View > Explore > nw/response/connector/threatconnect.</p>
<p>Workaround</p>	<p>You must perform the following actions after adding the SSL certificate to the Response Actions Server service trust-store.</p> <ul style="list-style-type: none"> - Adding the CommonName (CN) of the certificate as the host mapping in <code>/etc/hosts</code> file.


- Entering the CommonName (CN) of the certificate in the **host** field in 
(Admin) > Services > select the Response Actions Server service >   > View >
Explore >nw/response/connector/threatconnect.

NetWitness Response Actions Reference Information

This section is intended to help you understand the purpose and application of NetWitness Response Actions and Quick Actions view. For each view, there is a brief introduction and a What Do You Want To Do table with links to related procedures. In addition, the reference materials include workflows and Quick Looks to highlight important features in the user interface.

- [Response Actions View](#)
- [Quick Actions Option](#)

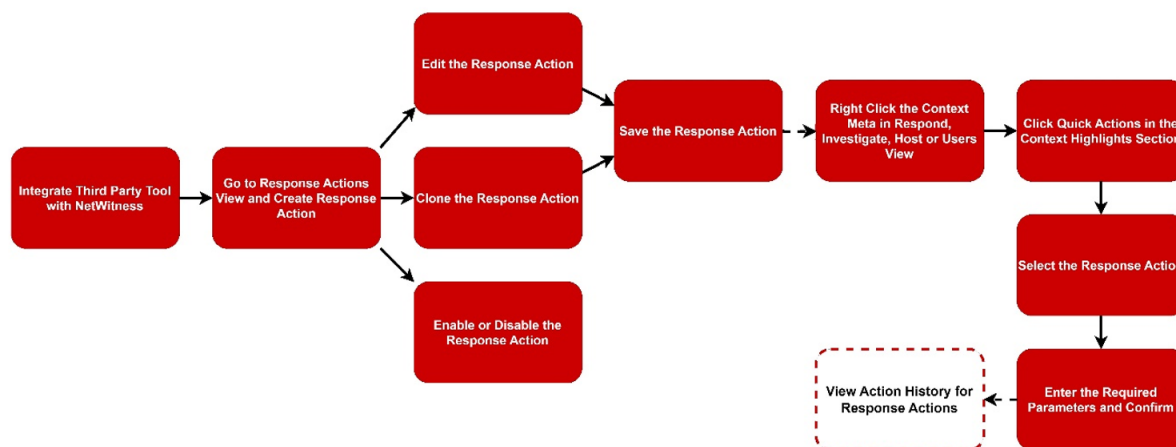
Response Actions View

Response Actions are the reactive operations performed on configured metadata using a third-party tool after triaging an event; the Response Actions feature ( (CONFIGURE) > **More** > **Response Actions**) allows you to integrate the supported third-party tools or connectors with the NetWitness platform and perform the following actions.

- Create and manage Response Actions for metas displayed in **Respond, Investigate, Hosts, and Users** views that support context highlights.
- Perform Quick Actions on the applicable meta and post the meta with additional information to the connector for taking further actions.

Workflow

The following figure is a high-level workflow illustrating the tasks you can do in the NetWitness Response Actions view.



What do you want to do?

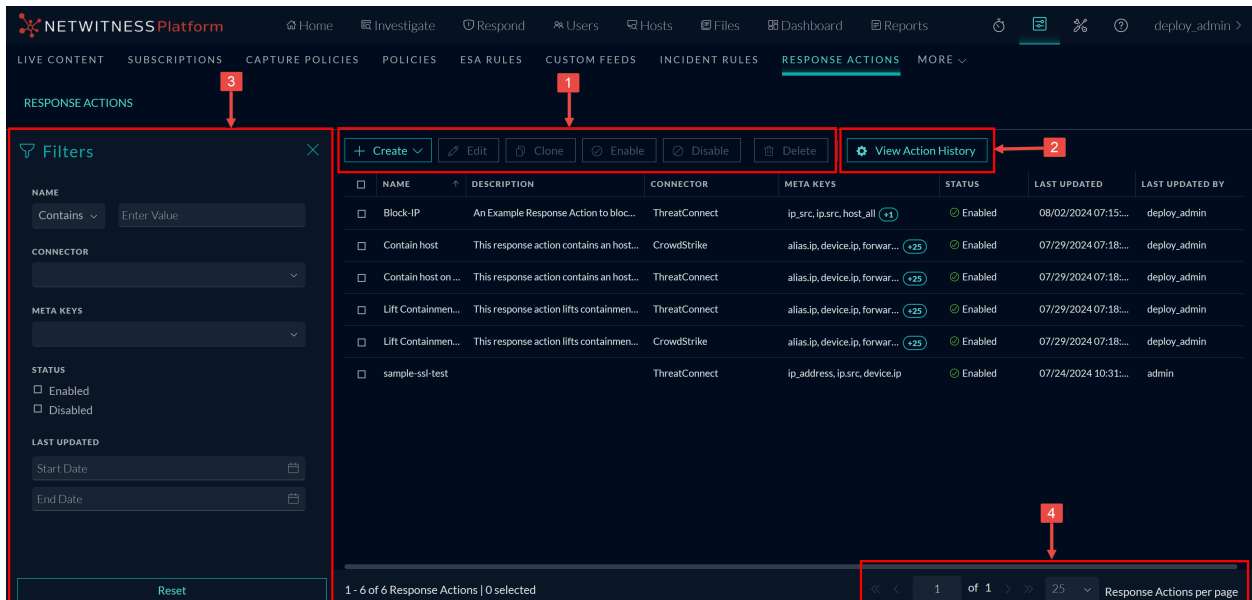
User Role	I want to ...	Show me how
Administrator	Create, edit, clone, enable, disable, delete, and view action history for Response Actions	Create and Manage Response Actions
Administrator	Filter Response Actions	See Response Actions Filters Panel in Quick Action History
Administrator	View and filter action history	Response Actions History View

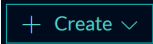
Related Topics

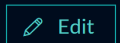
- [Integrate the Connector with NetWitness Platform](#)
- [Create and Manage Response Actions](#)
- [Quick Actions](#)
- [Connect with Threat Connect using HTTPS](#)
- [Response Actions and Quick Actions Use Case Examples](#)


Quick Look

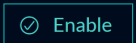
To access the Response Actions view, go to the ( (CONFIGURE) > More > Response Actions view.

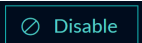


1 : Allows you to create a new Response Action. This option is grayed out if you have not integrated any connector with the NetWitness platform. If the connector is integrated with NetWitness Platform, you can select the same from the drop-down list.

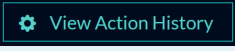



: Allows you to edit the existing Response Action.

: Allows you to clone the existing Response Action.

: Allows you to enable an already disabled Response Action.

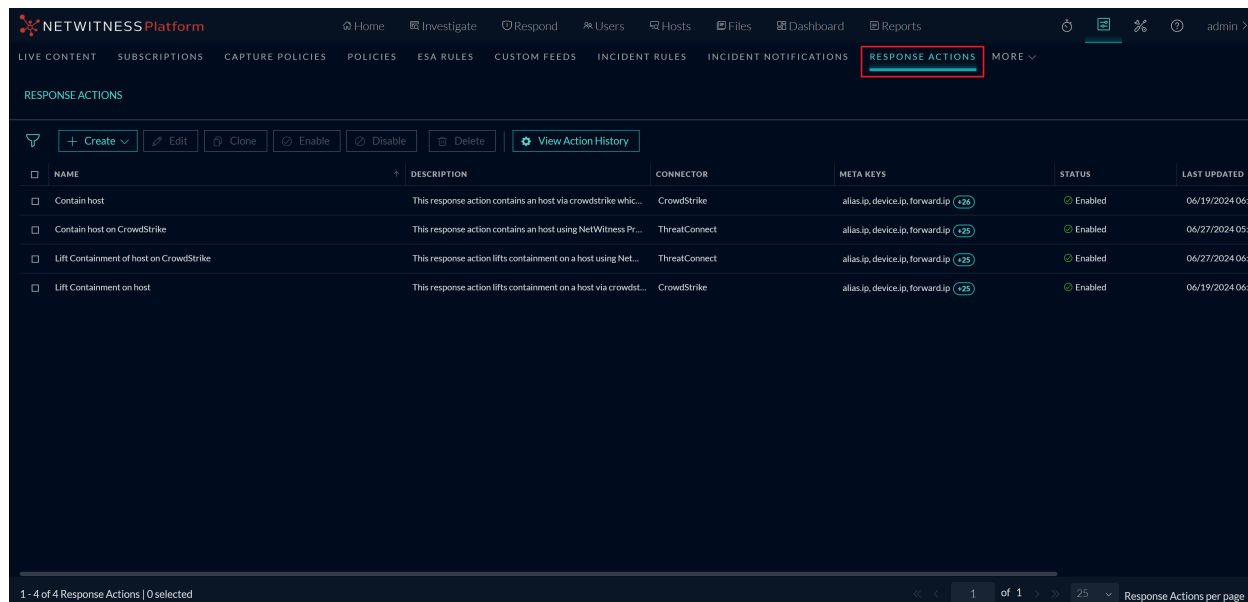
: Allows you to disable the selected Response Action.

: Allows you to delete the required Response Action.

- 2 : Allows you to view the history of the Response Actions.
- 3 : Allows you to filter and view the required Response Actions in the Response Actions List view.
- 4 By default, 25 Response Actions are displayed per page. To go to the next page, click . To go to the last page, click .

Response Actions List View

The Response Actions List displays all the Response Actions configured in the NetWitness Platform. You can filter this list to view only the Response Actions of interest.



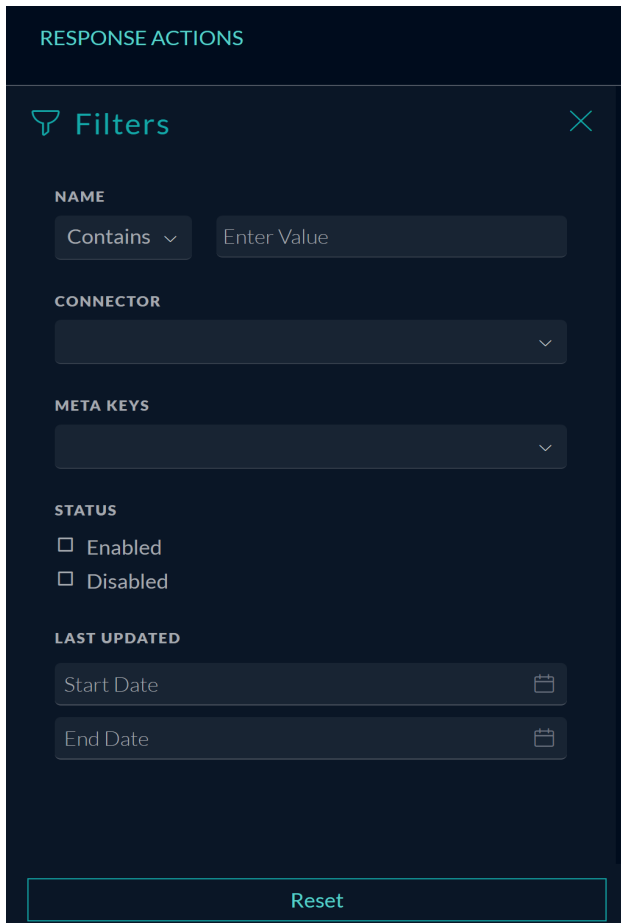
The following table describes the columns in the Response Actions List.

Columns	Description
Name	Displays the name of all the Response Actions in the Response Actions List view.
Description	Displays the descriptions of the Response Actions.
Connector	Displays the name of the third-party tool for which the particular Response Action is configured.
Meta Keys	Displays the list of meta keys for which the Response Action is supported.
Status	Displays the current status of the Response Action. For example: Enabled and Disabled .
Last Updated	Displays the date and time when the Response Action was last updated.

Columns	Description
Last Updated By	Displays the name of the user who updated the Response Action last time.

Response Actions Filters Panel

The following figure shows the filters available in the Response Actions **Filters** panel.



You can filter the Response Actions based on the following parameters.

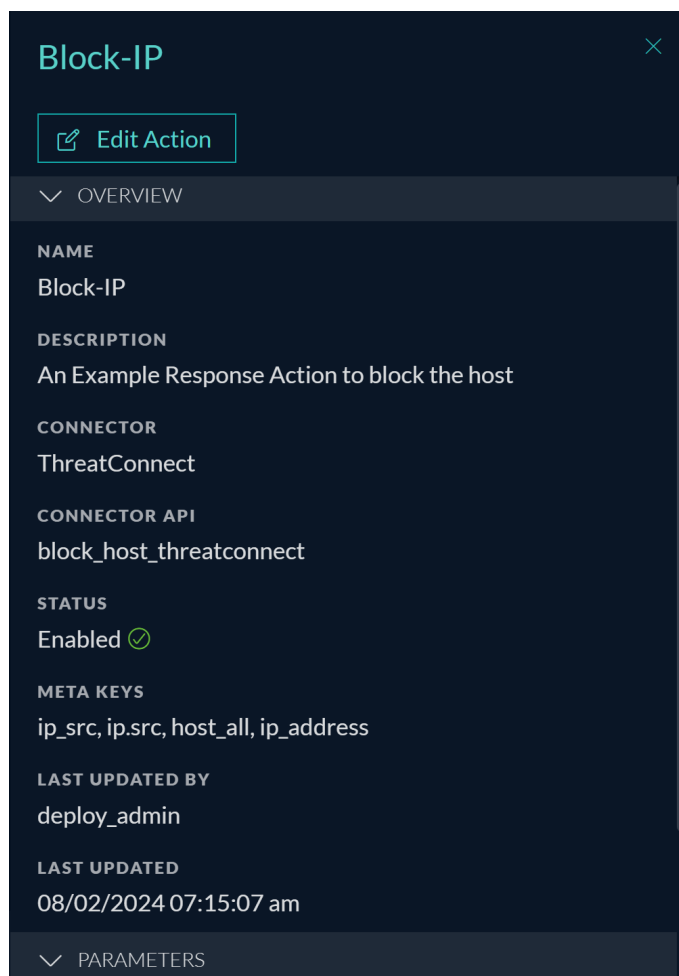
- Response Action Name
- Connector
- Status of the Response Action
- Supported Meta Keys
- Last updated Date and Time

The following table lists all the fields displayed in the Response Actions List view Filters panel.

Fields	Description
Name	Allows you to enter the name of the required Response Action.
Connector	Allows you to select the third party tool for which the particular Response Action was executed. For example: ThreatConnect or CrowdStrike
Status	Allows you to filter the Response Action based on the status Enabled or Disabled .
Meta Keys	Allows you to filter the Response Action based on the meta keys supported.
Last Updated	Allows you to filter the Response Action based on the date and time when the action was last updated.
Reset	Removes your existing filters.

Response Actions Overview panel


When you click any row in the Response Actions List, the Overview panel is displayed on the right side of the Response Actions List view, which shows the basic summary information about the particular Response Action.



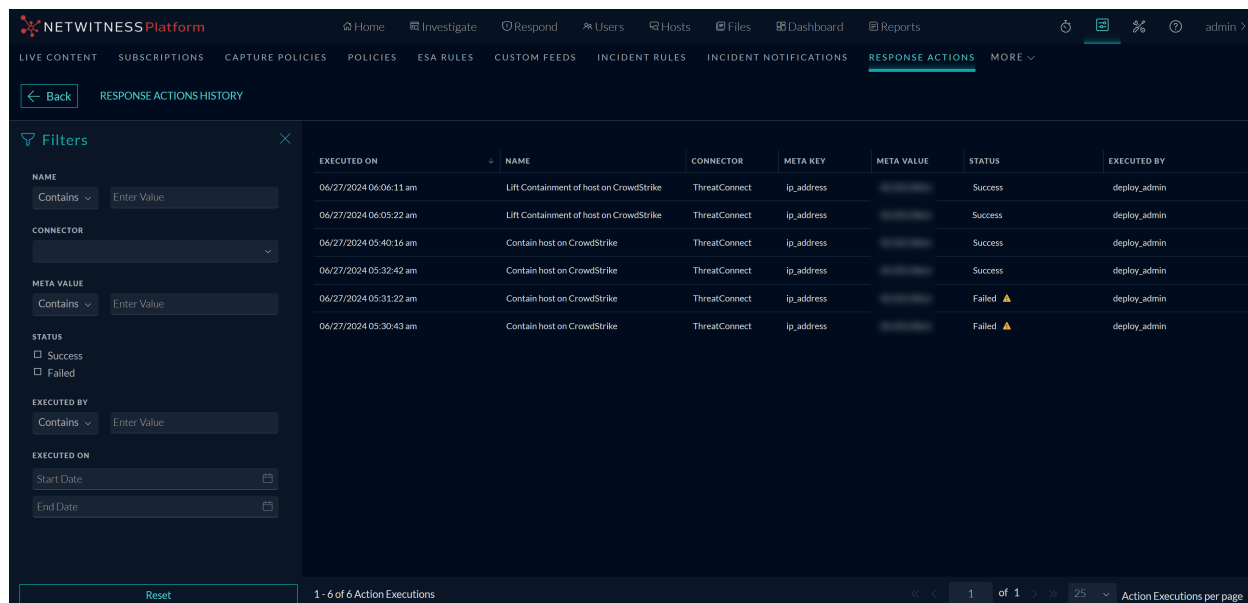
The following table displays the fields and parameters associated with the Overview panel.

Field Name	Description
Name	Displays the name of the Response Action executed. For example, Block IP
Description	Displays a brief description of what the response action contains.
Connector	Displays the connector name associated with the Response Action executed. For example, ThreatConnect or CrowdStrike .
Connector API	Displays the connector API details associated with the Response Action executed. For example, block-host-threatconnect .
Status	Displays the status of the Response Action executed. For example, Enabled.
Meta Keys	Displays the supported Meta Key for which the particular Response Action was executed. For example, ip.src and mac_address .
Last Updated By	Displays the name of the user who executed the Response Action last time.
Last Updated	Displays the Date and Time when the Response Action was last executed. For example, 12/19/2023 07:32:01 am
IP-Meta	Displays the meta value on which the quick action is performed.
Additional IP	Displays the additional IP details.

Response Actions History List view

When you execute Response Actions in the **Quick Actions**, the actions performed are recorded and the associated data is displayed in the **Response Actions History** view ( (CONFIGURE) > **More** > **Response Actions** > **View Action History** > **Response Actions History**). This is a global view of all actions performed across all Response actions.

The Response Actions History List displays the history of all the Response Actions executed in the NetWitness Platform.



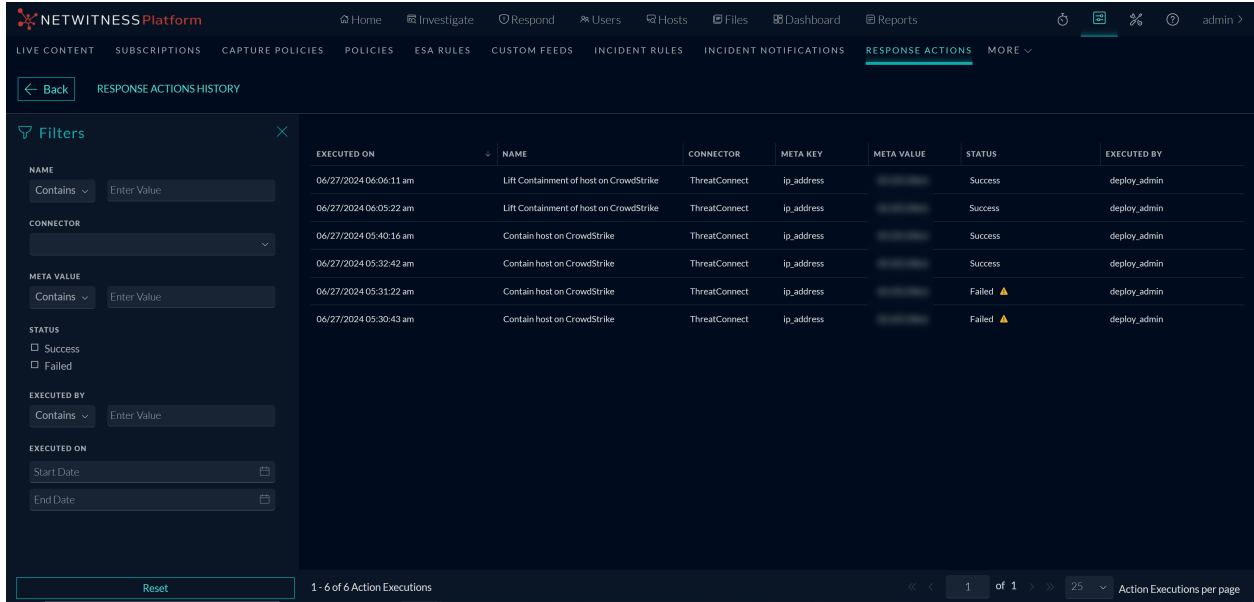
The following table describes the columns in the Response Actions History List view.

Columns	Description
Executed On	Displays the date and time when the Response Action was last executed. For example: 12/11/2023 05:06am
Name	Displays the name of all the Response Actions executed.
Connector	Displays the name of the third party tool for which the particular Response Action was executed. For example: ThreatConnect or CrowdStrike
Meta Key	Displays the list of meta keys for which the Response Action was executed. For example: ip.src
Meta Value	Displays the value of the meta key for which the Response Action was executed. For example: 10.125.237.89
Status	Displays the status of the execution of Response Action. For example: Success and Failed .

Executed By Displays the name of the user who executed the Response Action last time.

Response Actions History Filters Panel

The following figure shows the filters available in the Response Actions History **Filters** panel.



You can filter the Response Actions based on the following parameters.

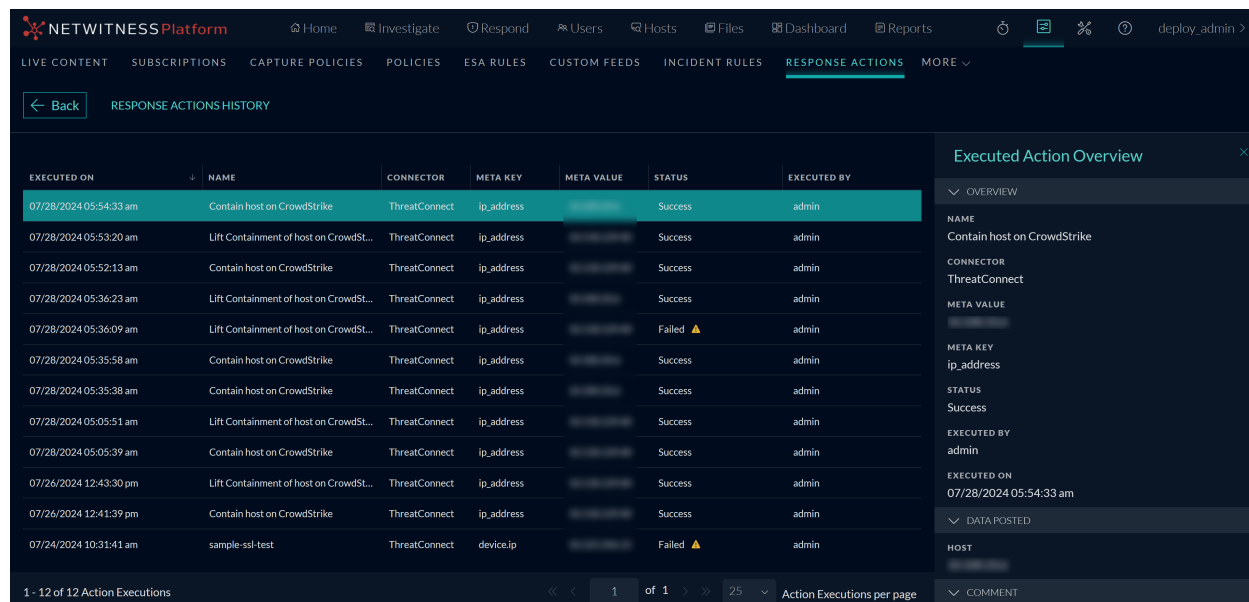
- Response Action Name
- Connector
- Status of the Response Action
- Supported Meta Keys
- Last updated Date and Time

The following table lists all the fields displayed in the Response Actions List view Filters panel.

Fields	Description
Name	Allows you to enter the name of the required Response Action.
Connector	Allows you to select the third party tool for which the particular Response Action was executed. For example: ThreatConnect or CrowdStrike
Status	Allows you to filter the Response Action on the basis of the status. For example, you can select Enabled or Disabled status to filter the required Response Action.
Meta Keys	Allows you to filter the Response Action on the basis of the meta keys supported.
Last Updated	Allows you to filter the Response Action based on the date and time when the action was last updated.
Reset	Removes your existing filters.

Response Actions History Overview panel

When you click any row in the Response Actions History List, the **Overview** panel is displayed on the right side of the **Response Actions History** view, which shows the basic summary information about the particular Response Action executed. The following fields and parameters are displayed in the Overview panel.



The following table lists all the fields displayed in the Response Actions History Overview view panel details.

Field Name	Description
Name	Displays the name of the Response Action executed. For example, If you provided Block IP as the Response Action name while executing the Response Action, the same Block IP name will be displayed in the Name field in the Response Actions History Overview panel.
Connector	Displays the connector name associated with the Response Action executed. For example, ThreatConnect or CrowdStrike .
Meta Value	Displays the meta value associated with the Meta Key. For example, If the supported Meta Key is ip.src , the meta value will be displayed in the form of an IP address such as 10.125.246.29 .
Meta Key	Displays the supported Meta Key for which the particular Response Action was executed. For example, ip.src and mac_address .
Status	Displays the status of the Response Action executed. For example, If the meta key and the additional parameters are forwarded to the connector successfully, the Status field displays Success . If the meta key and the additional parameters are not forwarded.

Field Name	Description
Executed By	Displays the name of the user who executed the Response Action last time.
Executed On	Displays the Date and Time when the Response Action was last executed. For example, 12/19/2023 07:32:01 am .
Additional Parameters	Displays the Parameter Key and Parameter Label that are posted to the connector. For example, the Data Posted section in the Response Actions History Overview panel displays the meta keys and additional parameters posted to ThreatConnect.
Comment	Displays the comment provided during the execution of the Response Action. For example, Post the parameters and the meta key to ThreatConnect.

Quick Actions Option

The **Quick Actions** option in the **Context Highlights** section allows users to use the response action configured for any applicable meta. Users can send the metadata, along with additional parameters, to a third-party tool for further processing.

This option is available when you right-click any context meta in the **Investigate**, **Respond**, **Users**, and **Hosts** view where Context Highlights appear.

What do you want to do?

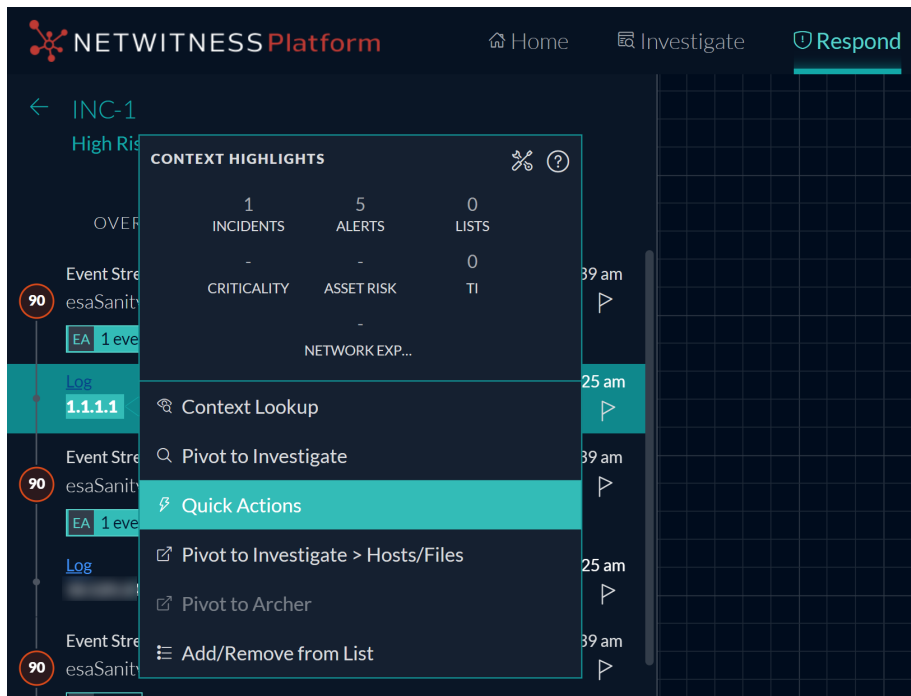
User Role	I want to ...	Show me how
Analysts	Perform Quick Actions	Quick Actions

Related Topics

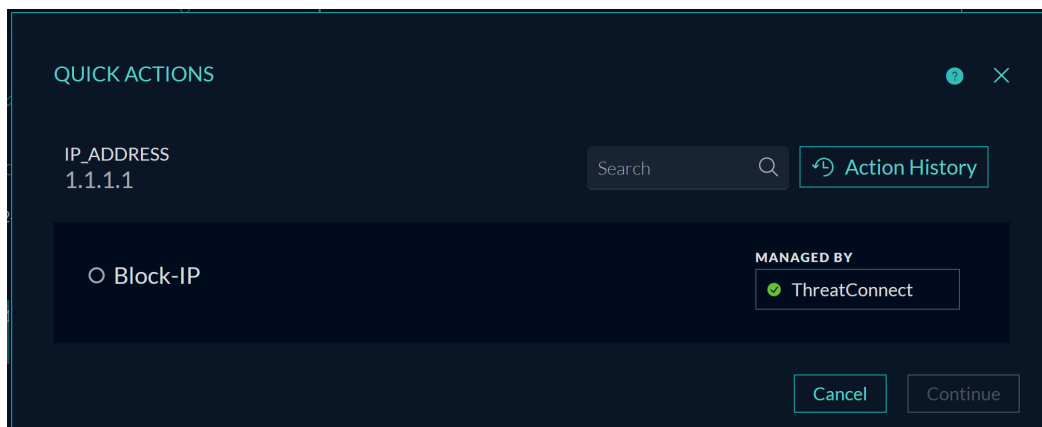
- [Create and Manage Response Actions](#)
- [Response Actions and Quick Actions Use Case Examples](#)

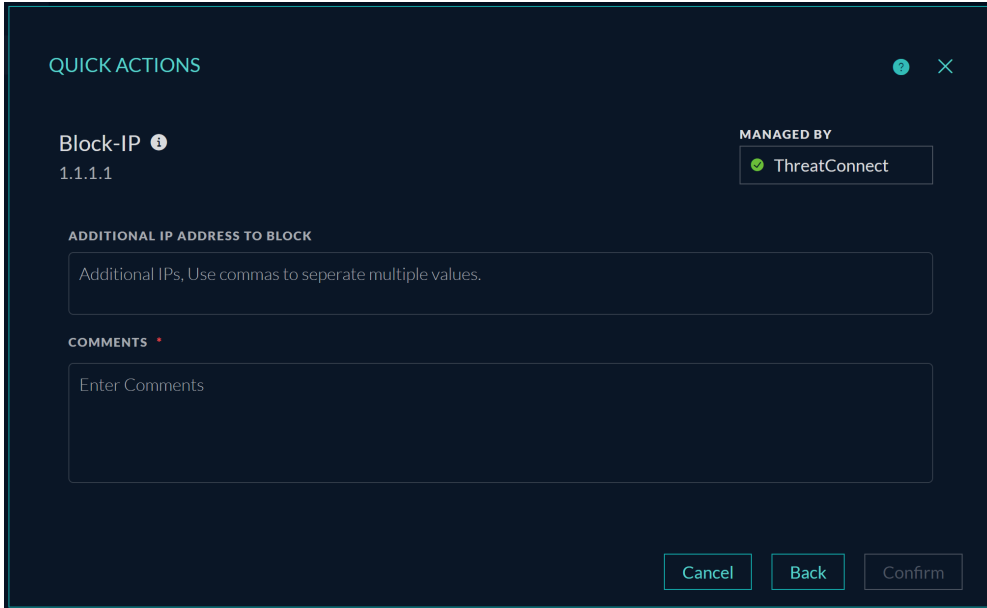
Quick Look

The following is an example of Quick Action from the Respond view.



The following figure shows the Quick Actions workflow.



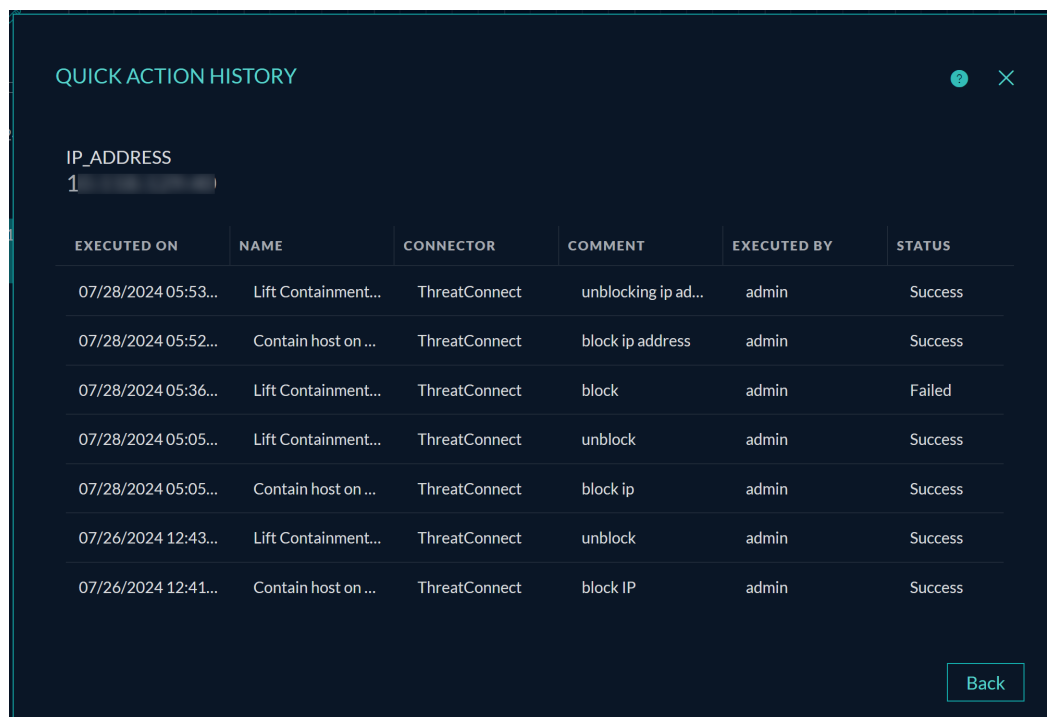
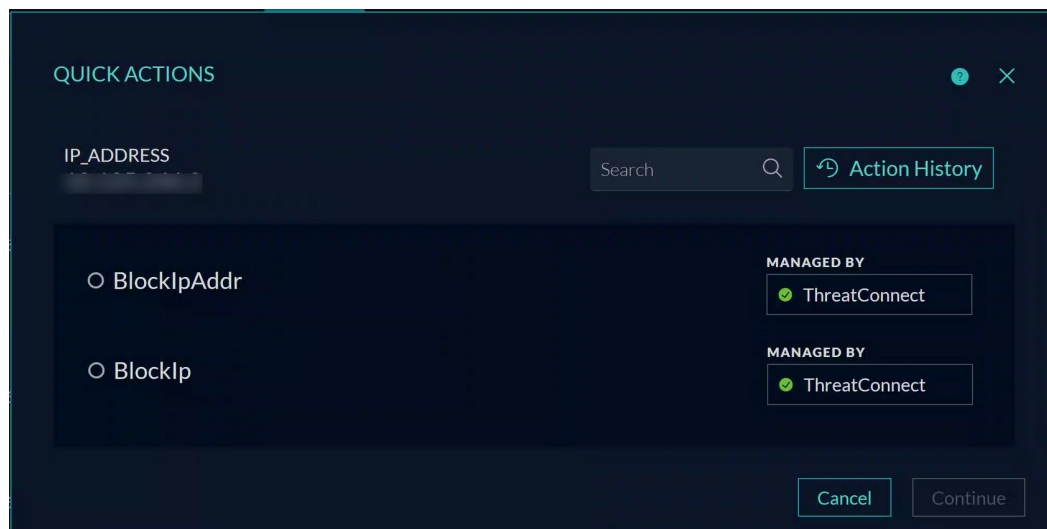


The following table describes the fields in the **Quick Actions** Panel.

Fields	Description
Search	Allows you to quickly search for the specific meta value.
Action History	Allows you to view the historical details of the Response Actions executed for that specific meta value.
Continue	Allows you to continue the configuration.
Parameter Label (Additional IP Address to Block)	Allows you to enter the parameter label value, added as part of the Response Actions screen, which is reflected as an Additional IP Address to Block field in the Quick Actions panel. For example, 1.1.1.0/24
Comments	Allows you to enter the comments while executing the Response Action.
Cancel	Closes the dialog without applying changes.
Back	Allows to navigate back to the previous screen.
Confirm	Applies the changes.

Quick Actions History View

When you click the **Action History** option in the **Quick Actions** window, the **Quick Action History** dialog displays the historical details of the Response Actions executed for that specific meta value.



The following table describes the columns in the **Quick Action History** view.

Columns	Description
Executed On	Displays the date and time when the Response Action was last executed. For example: 12/11/2023 05:06 am
Name	Displays the name of all the Response Actions executed.
Connector	Displays the name of the third-party tool for which the particular Response Action was executed. For example, ThreatConnect

Columns	Description
Comment	Displays the comment provided while executing the Response Action.
Executed By	Displays the name of the user who executed the Response Action last time.
Status	Displays the status of the execution of Response Action. For example, Success and Failure.