

# NetWitness<sup>®</sup> Platform XDR

Version 12.1.0.0

## Live Services Management 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 and 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.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

March, 2023

# Contents

---

<b>Live Services Management</b> .....	<b>8</b>
NetWitness Live .....	8
NetWitness Feedback and Data Sharing .....	8
For Debian Linux and NetWitness Endpoint Users .....	8
<b>Deploy Content</b> .....	<b>9</b>
Create Live Account .....	10
Reset the Password for Your Live Account .....	13
Set Up Live Services on NetWitness Platform XDR .....	14
Deploy Content using Live Content UI .....	16
Live Services Required Procedures .....	17
Find and Deploy Live Resources .....	18
Find Resources in Live .....	18
Deploy Resources in Live .....	19
Manage Live Resources .....	25
Manage Subscription and Deployment .....	25
Remove a Deployed Resource .....	26
Deploy a Resource Bundle .....	26
Download Resources .....	26
Set Up Data Feeds .....	26
Search and Download Content from NetWitness XDR Cloud Services Live .....	27
Quick Search for Content .....	27
Advanced Search for Content .....	28
Download Content .....	29
Additional Procedures .....	32
Export Data to RSA .....	33
About Live Feedback .....	33
Download Live Feedback Historical Data .....	33
Share Telemetry Data to NetWitness .....	33
Packaging Resources .....	35
Create and Deploy Resource Package Use Case .....	35
Prerequisites to Create a Resource Package .....	35
Creating a Resource Package .....	35
Creating Threat Package .....	36
Deploying a Threat Package .....	37
Manage Custom Feeds .....	39
Custom Feed Creation .....	39
Sample Feed Definition File .....	39
Feed Definition Equivalents for Custom Feed Wizard Parameters .....	40
Creating a Custom Feed .....	43
Import Certificates for HTTPS Service .....	49

Create a STIX Custom Feed .....	51
MetaCallback Feeds using CIDR Index Range for IPv4 and IPv6 .....	56
Creating and Managing an Identity Feed .....	57
Import the SSL Certificate .....	64
Cannot Verify Identity Feed URL .....	64
Investigating an Identity Feed .....	65
Editing a Feed .....	67
Removing a Feed .....	69
Subscribing to Live Resources .....	71
Subscription Updates .....	71
Adding Subscribed Resources for Deployment to Services .....	72
Deleting a Subscription .....	72
Removing Subscribed Resources from the Deployments Subscriptions Grid .....	73
Subscribe and Unsubscribe to a Resource .....	73
Viewing Subscribed Resources Selected to Deploy on Services .....	75
Miscellaneous Live Services Procedures .....	76
Displaying Resource Details in Live Resource View .....	76
Downloading a Resource .....	77
Locating and Removing a Deployed Resource from Services .....	77
Showing Results as a List or in Detail .....	78
Viewing Resource Details .....	79
References .....	81
Live Configure View .....	82
Deployments Tab .....	83
Groups Panel .....	83
Subscriptions Panel .....	84
Subscriptions Tab .....	85
Toolbar .....	85
Grid .....	86
Discontinued Resources Tab .....	87
Groups Panel .....	87
Discontinued Resources on Service Panel .....	88
Live Feeds View .....	89
Toolbar .....	89
Feeds Grid .....	90
Live Resource View .....	91
Resource Details .....	91
Resource View Toolbar .....	92
Live Search View .....	94
Search Criteria Panel .....	94
Matching Resources Panel .....	97
Detailed Results .....	97

Grid Results .....	98
See Also .....	99
Live Search Content View .....	100
Search Content Panel .....	101
Search Results Panel .....	103
Content Details Panel .....	104
Resource Package Deployment Wizard .....	107
Features .....	107
Package Tab .....	107
Resources Tab .....	108
Services Tab .....	108
Review Tab .....	109
Deploy Tab .....	110
NetWitness Live Registration Portal .....	112
NetWitness Feedback and Data Sharing .....	114
Additional Live Services .....	114
Live Feedback .....	114
File Reputation .....	114
Troubleshooting Live Services .....	116
OutOfMemoryError on Context Hub Server .....	116
Troubleshooting Live Connect Threat Data Sharing .....	116
Query Log Retrieval Sample .....	117
System Logging: Debug .....	117
Policy-based Centralized Content Management .....	119
About Policy-based Centralized Content Management (CCM) .....	122
Workflow .....	123
Benefits .....	123
Enable or Disable CCM for All or Individual Services .....	125
How to Enable or Disable CCM for All Services .....	125
How to Enable or Disable CCM for Individual Services .....	126
Manage Content Library .....	126
Migrate Content from Core Services to Content Library .....	127
Import Content to Content Library .....	129
Create an Application Rule .....	129
Clone Application Rule .....	130
Edit Application Rule .....	131
Delete Application Rule .....	131
View Application Rule Details .....	132
Create a Network Rule .....	132
Clone Network Rule .....	133
Edit Network Rule .....	134
Delete Network Rule .....	134

View Network Rule Details .....	135
Create an ESA Rule .....	135
Edit an ESA Rule .....	135
Delete an ESA Rule .....	136
Filter Content Rules .....	136
Manage Groups .....	138
Create a Group .....	138
View a Group .....	139
Delete a Group .....	139
Edit a Group .....	140
Filter Groups .....	141
Manage Policies .....	142
Create and Publish Policies .....	142
Clone a Policy .....	146
Delete a Policy .....	146
Edit a Policy .....	147
View a Policy .....	147
Enable Content for a Policy .....	149
Disable Content for a Policy .....	149
Filter Policies .....	150
Filter Policy Content Details .....	151
Merge Policy with ESA Content .....	153
Manage ESA Datasources .....	154
View an ESA Datasource .....	155
Add an ESA Datasource .....	155
Edit an ESA Datasource .....	157
Delete an ESA Datasource .....	158
Manage Deployments .....	158
View a Deployment .....	159
Create a Deployment .....	161
Edit a Deployment .....	169
Start a Deployment .....	172
Remove a Deployment .....	174
Stop a Deployment .....	175
Migrate ESA Deployments to Policies and Groups .....	177
References .....	179
Content Library Tab .....	179
Data Sources Tab .....	184
Deployments Tab .....	187
Groups Tab .....	191

Policies Tab .....	195
Appendix A: Endpoint Risk Scoring Rules .....	201
Appendix B: Position Tracking Information .....	217
Use Case Scenario .....	217

# Live Services Management

---

NetWitness Live is the gateway to a rich environment that offers access to feeds, tools, and other resources.

## NetWitness Live

Live is the component of NetWitness that manages communication and synchronization between NetWitness services and a library of Live content available to NetWitness customers. Live provides a simple interface for browsing, selecting, and deploying content from the NetWitness Live Content Management System to NetWitness services and software. In addition to managing feeds from the CMS Library, Live allows users to deploy custom feeds and packages.

**Note:** Any customer with valid maintenance can access NetWitness Live.

The content management system (CMS) library (known as *Live*) is a valuable source of the latest internet security resources for NetWitness customers. It provides a view into the collective intelligence and analytical skills of the worldwide security community to ensure that users have the most current visibility into attack vectors.

Live gathers the best advanced threat intelligence and content in the global security community - the ideas, research, ongoing tracking, and analysis - and brings it directly into the user's security operations center to definitively classify computers associated with botnets, malware, and other malicious exploits. Live aggregates, consolidates, and illuminates only the most pertinent information relevant to an organization on a real-time basis.

## NetWitness Feedback and Data Sharing

**Live Feedback** is intended to help improve NetWitness. Once you set up and configure a Live account, usage data is shared with RSA.

For more details, see [NetWitness Feedback and Data Sharing](#).

## For Debian Linux and NetWitness Endpoint Users

If you are upgrading to NetWitness 11.5 or later, and you are using NetWitness Endpoint and also have any Debian Linux endpoint systems, NetWitness recommends that you go to Live and download the following application rules:

- autorun debian package mismatch
- autorun file path not part of debian package
- debian package hash mismatch in important system directory
- debian package hash mismatch
- file path not part of debian package in important system directory
- file path not part of debian package



## Deploy Content

---

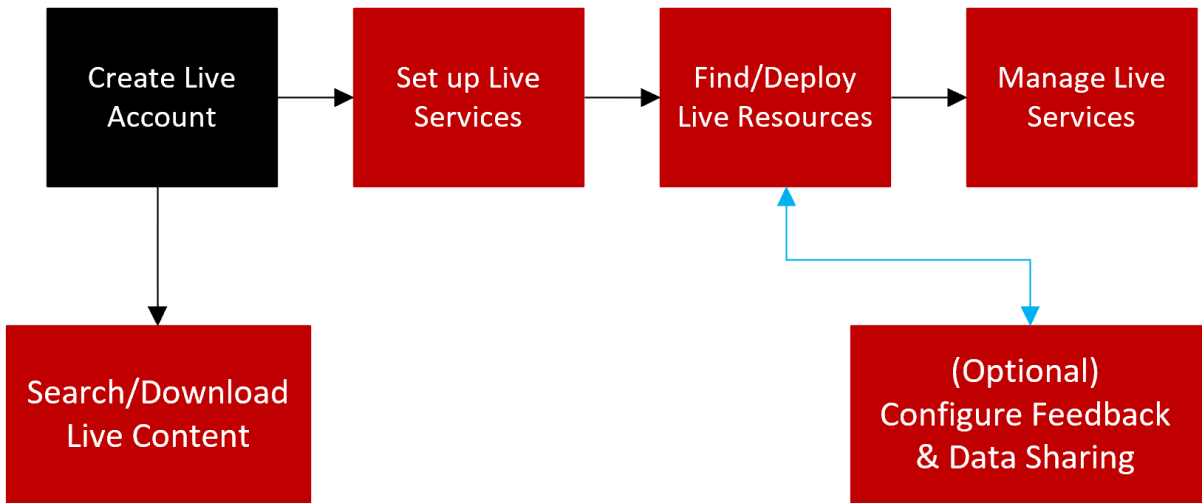
This section explains the different ways available to deploy content:

- [Deploy Content using Live Content UI](#)
- [Policy-based Centralized Content Management](#)


## Create Live Account

**Note:** The NetWitness Live Registration Portal now has a new user interface and supports email verification.

You must create a Live account using the NetWitness Live Registration Portal (<https://live.netwitness.com/registration>) on the Live server. Live Account is required to access all Live services including CMS. The CMS Library provides access to all NetWitness content in one place where you can view, search, deploy, and subscribe to NetWitness content.



Make sure the following are available to set up a NetWitness Live account:

- Active internet connection to access the portal.
- A valid and registered NetWitness License Server on the Flexera Server, before you can register for a Live account. You can view the License ID on the  (Admin) > System > Info panel.

**Note:** If the License Server is not set up, contact [NetWitness Customer Support](#).

### To create a Live Account:

1. Access the NetWitness XDR Cloud Services Live Registration Portal using the URL: <https://live.netwitness.com/registration>

The NetWitness XDR Cloud Services Live sign up page is displayed.



**NETWITNESS**  
XDR Cloud Services

**Sign in with your username and password**

Username \*

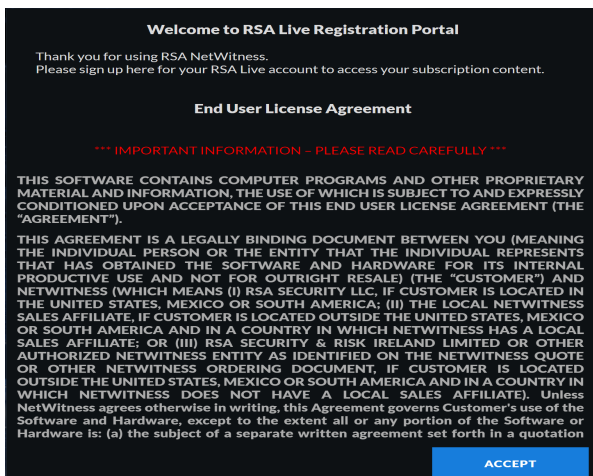
Password \*

**SIGN IN**   **SIGN UP FOR LIVE**   [Forgot Password?](#)

2. Click **Sign Up For Live**.

The End User License Agreement page is displayed.

Read the Terms and Conditions carefully and click **Accept**.



**Welcome to RSA Live Registration Portal**

Thank you for using RSA NetWitness.  
Please sign up here for your RSA Live account to access your subscription content.

**End User License Agreement**


**\*\*\* IMPORTANT INFORMATION - PLEASE READ CAREFULLY \*\*\***

THIS SOFTWARE CONTAINS COMPUTER PROGRAMS AND OTHER PROPRIETARY MATERIAL AND INFORMATION, THE USE OF WHICH IS SUBJECT TO AND EXPRESSLY CONDITIONED UPON ACCEPTANCE OF THIS END USER LICENSE AGREEMENT (THE "AGREEMENT").

THIS AGREEMENT IS A LEGALLY BINDING DOCUMENT BETWEEN YOU (MEANING THE INDIVIDUAL PERSON OR THE ENTITY THAT THE INDIVIDUAL REPRESENTS THAT HAS OBTAINED THE SOFTWARE AND HARDWARE FOR ITS INTERNAL PRODUCTIVE USE AND NOT FOR OUTRIGHT RESALE) (THE "CUSTOMER") AND NETWITNESS (WHICH MEANS (I) RSA SECURITY LLC, IF CUSTOMER IS LOCATED IN THE UNITED STATES, MEXICO OR SOUTH AMERICA; (II) THE LOCAL NETWITNESS SALES AFFILIATE, IF CUSTOMER IS LOCATED OUTSIDE THE UNITED STATES, MEXICO OR SOUTH AMERICA AND IN A COUNTRY IN WHICH NETWITNESS HAS A LOCAL SALES AFFILIATE; OR (III) RSA SECURITY & RISK IRELAND LIMITED OR OTHER AUTHORIZED NETWITNESS ENTITY AS IDENTIFIED ON THE NETWITNESS QUOTE OR OTHER NETWITNESS ORDERING DOCUMENT, IF CUSTOMER IS LOCATED OUTSIDE THE UNITED STATES, MEXICO OR SOUTH AMERICA AND IN A COUNTRY IN WHICH NETWITNESS DOES NOT HAVE A LOCAL SALES AFFILIATE). Unless NetWitness agrees otherwise in writing, this Agreement governs Customer's use of the Software and Hardware, except to the extent all or any portion of the Software or Hardware is: (a) the subject of a separate written agreement set forth in a quotation

**ACCEPT**

3. In the **Sign Up for NetWitness Live Account** page, enter all the fields:

- The **First Name** and **Last Name** of the user.
- The **Company** for which the Live Account is being created.
- The **Email address** you enter will be used to receive the verification code for your new Live account and other notifications related to the Live account.
- The **License ID** can be viewed on  (**Admin**) > **System** > **Info** panel.

- The **Username** and **Password** for the Live Account.



The screenshot shows the 'Sign Up for NetWitness Live Account' page. At the top, the NetWitness logo is displayed with the text 'NETWITNESS' and 'XDR Cloud Services' below it. The main heading is 'Sign Up for NetWitness Live Account' with a help icon. The form contains several input fields with their respective labels and validation rules:

- First Name:** Only Alphabets; Length:[3,16]
- Last Name:** Only Alphabets; Length:[3,16]
- Company:** Alphanumeric with Space; Start with Alpha; Length:[2,16]
- Email:** In case of account recovery and communications
- License ID:** Look in System/Administration Page
- Username:** Alphanumeric with . and \_; Start with Alpha; Length:[4,16]
- Password:** Number,lower,UPPER,~!@#%&\*()\_+./; Length:[8,24]

At the bottom of the form, there are two buttons: 'Back to Sign In' and 'CREATE ACCOUNT'.

4. Click **Create Account**.  
You will be directed to **Confirm Sign up** page.
5. Enter the **Confirmation Code** sent to your registered email address.  
Click **Confirm**.  
You can see the confirmation message for your NetWitness Live Account registration.

**Note:** You cannot create more than one Live account for the same License ID. For additional license, contact [NetWitness Customer Support](#).

6. Once the account is created, enter your credentials and click **Sign In** to access the NetWitness XDR Cloud Services Live.
7. After you sign in, you can perform the following:
  - [Search and Download Content from NetWitness XDR Cloud Services Live](#)
  - [Share Telemetry Data to NetWitness](#)

## Reset the Password for Your Live Account

If you want to reset the password for your Live Account, do the following:

1. Access the NetWitness XDR Cloud Services Live Registration Portal using the URL:


<https://live.netwitness.com/registration>

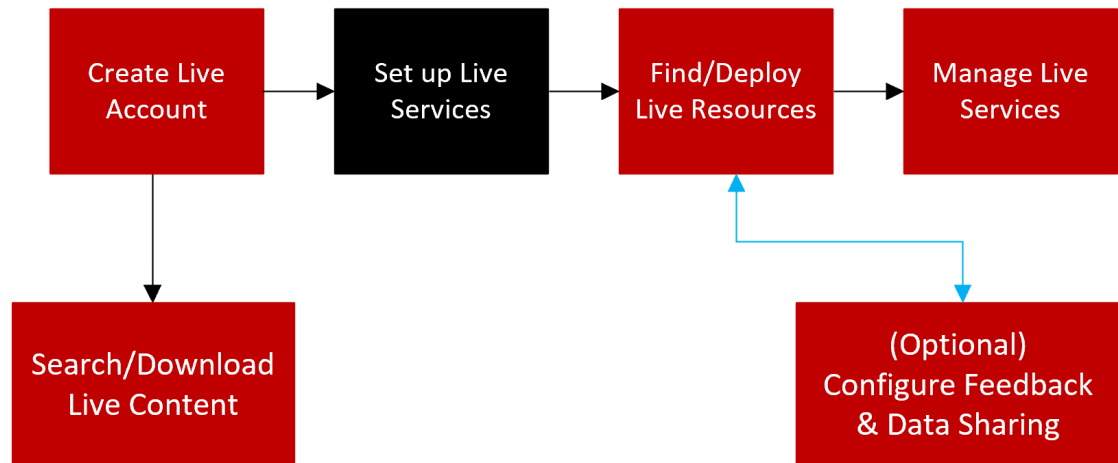
The NetWitness XDR Cloud Services Live sign up page is displayed.




2. On the Sign Up page, click **Forgot Password?**.
3. Enter your **Username** and click **Send Code**.  
A verification code will be sent to your registered email address.
4. Enter the **Verification Code** and **New Password** on the Reset Password page and click **Submit**.

## Set Up Live Services on NetWitness Platform XDR

To set up Live on NetWitness Platform XDR, you configure the connection and synchronization between the CMS server and NetWitness. The user interface for this setup is the  (Admin) > System > Live Services Configuration panel.



### To configure the connection to the CMS Server:

1. Navigate to  (Admin) > System > Live Services.
2. Click Sign In and enter your credentials in the Live Services Account dialog box.

Live Services Account

Host: cms.netwitness.com

Port: 443

SSL:

Username: admin

Password: \*\*\*\*\*

Test Connection

Cancel Apply

3. Click Test Connection to make sure your connection is working.

4. If the test is successful, click **Apply**. If not, contact [NetWitness Customer Support](#) for help connecting to the Live server.
5. Configure the timing for synchronization of NetWitness Platform XDR with updates from Cloud Services Live.

For more details, see the "Configure Live Services Settings" topic in the *System Configuration Guide*.

## Deploy Content using Live Content UI

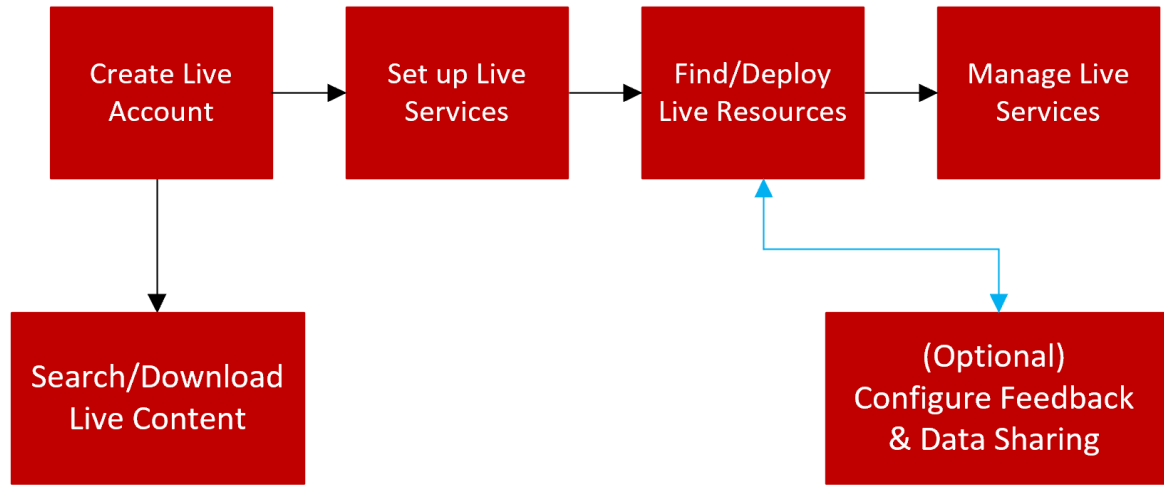
This topic explains the process of deploying the content using Live Content UI.

- [Live Services Required Procedures](#)
- [Additional Procedures](#)
- [References](#)
- [Troubleshooting Live Services](#)



## Live Services Required Procedures

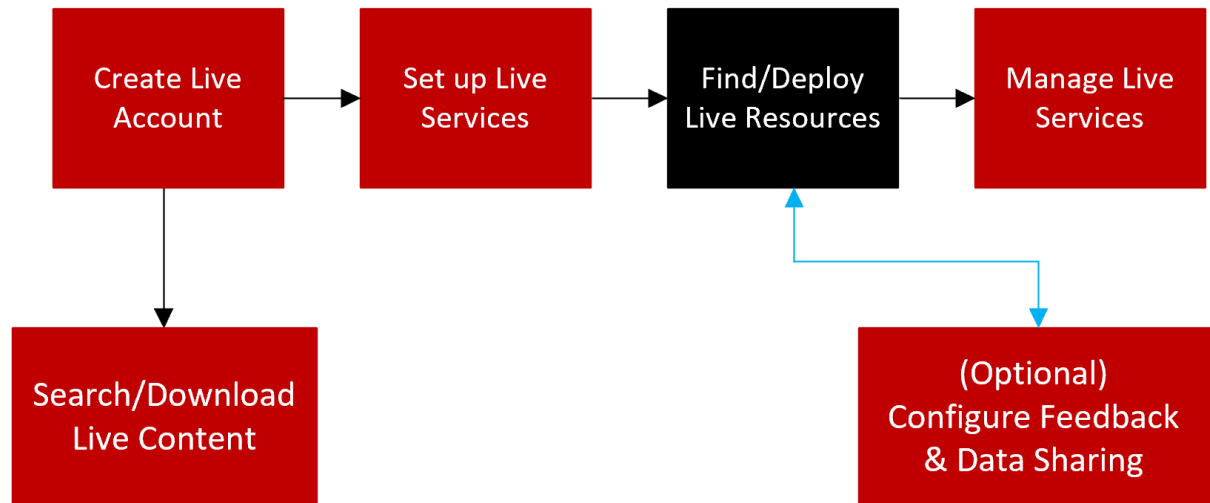
The following workflow describes the basic setup into four steps, which you perform individually.



Configuration Step	Description
<a href="#">Create Live Account</a>	Create a Live Account on the Cloud Services Live Registration portal URL: <a href="https://live.netwitness.com/registration">https://live.netwitness.com/registration</a> .
<a href="#">Set Up Live Services on NetWitness Platform XDR</a>	Set Up Live Services on NetWitness Platform XDR by configuring a connection with the CMS server.
<a href="#">Find and Deploy Live Resources</a>	Search and browse for resources in the Live Search view, and then, deploy the selected resources.
<a href="#">Manage Live Resources</a>	Procedures for administrators to search for, subscribe to, and deploy resources from Live.
<a href="#">Search and Download Content from NetWitness XDR Cloud Services Live</a>	Search and browse for content in the Cloud Services Live, and then, download the selected content.
<a href="#">NetWitness Feedback and Data Sharing</a>	Describes the feedback and data sharing features provided in NetWitness, from Live Services. Participation is optional, but can help to provide useful threat intelligence for the community.

## Find and Deploy Live Resources


Administrators can search for resources in the Live Search view, which is also the same as browsing the Live CMS for resources using the Search Criteria panel of the [Live Search View](#).



### Find Resources in Live

**IMPORTANT:** ESA Rules cannot be deployed manually via Live Services. By default, all the ESA rules are available in the ESA Rule library if Live Service is configured.

#### To find resources:

1. Navigate to  (Configure) > Live Content.
2. In the **Search Criteria** panel, specify search criteria. Enter any or all of these: keyword, category, type of resource, medium, meta keys, meta values, date resource was created, and date resource was modified.

### 3. Click **Search**.

The Matching Resources panel displays detailed results.

### 4. (Optional) To further narrow the results In the Matching Resources panel, click on a tag, meta key, medium or resource meta value in a result.


## Deploy Resources in Live

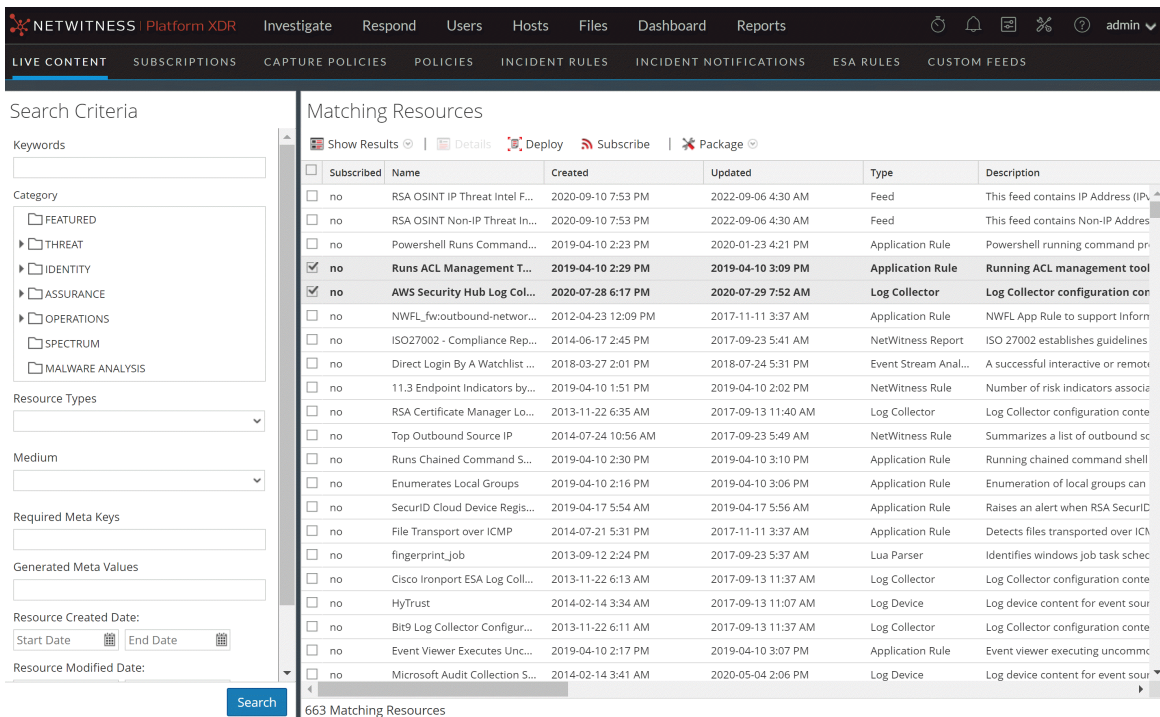
In NetWitness, you can deploy selected resources manually, using the Deployment Wizard, or you can subscribe to a group of resources.

- When you have results from browsing resources in NetWitness Live, you can deploy resources manually to a service or a service group without subscribing to the resources. To deploy resources, select one or more from the list.
- Deploying resources manually deploys to services without taking advantage of the powerful resource management capabilities of NetWitness. If you want to receive notification and updates for updated resources and be able to easily remove resources from a service, you must subscribe to resources in the Live Search view and deploy them in the [Live Configure View](#).
- If you have previously created and saved a resource package, you can deploy the package to services. Please refer to [Resource Package Deployment Wizard](#) for instructions on how to create a package.

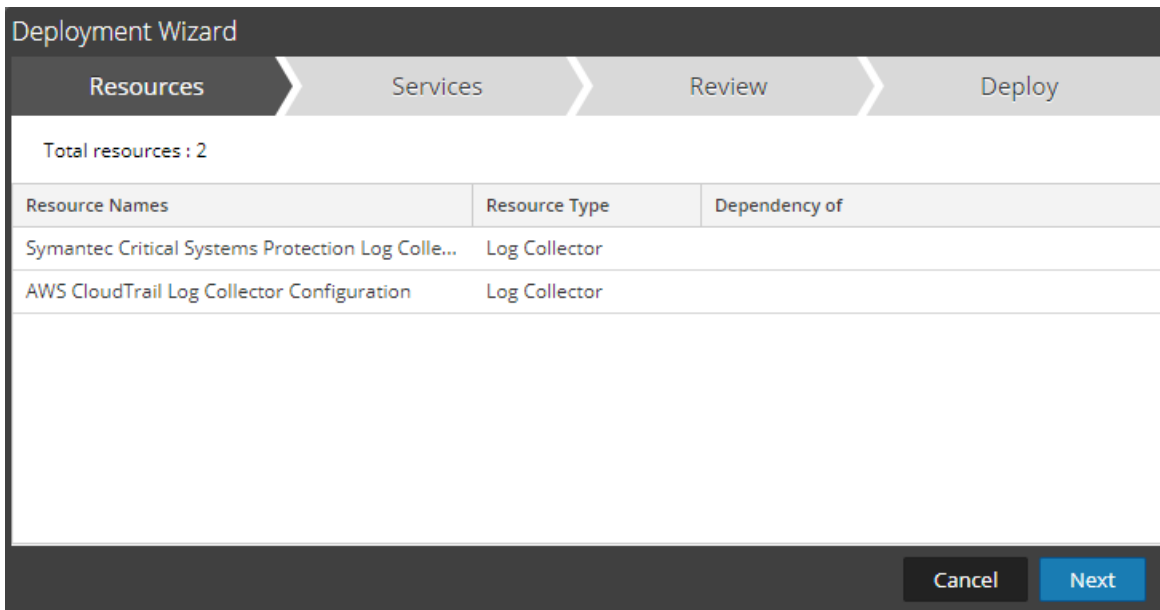
**Caution:** For NetWitness 11.3, there is a new Content bundle for Endpoint, which contains approximately 400 application rules. Do not deploy this bundle (or the Endpoint application rules) onto any Log Decoder that is running an earlier version of NetWitness. The rules are only useful for 11.3 and newer, and would have major performance implications if deployed on Log Decoders that cannot process them.

### To deploy resources manually:

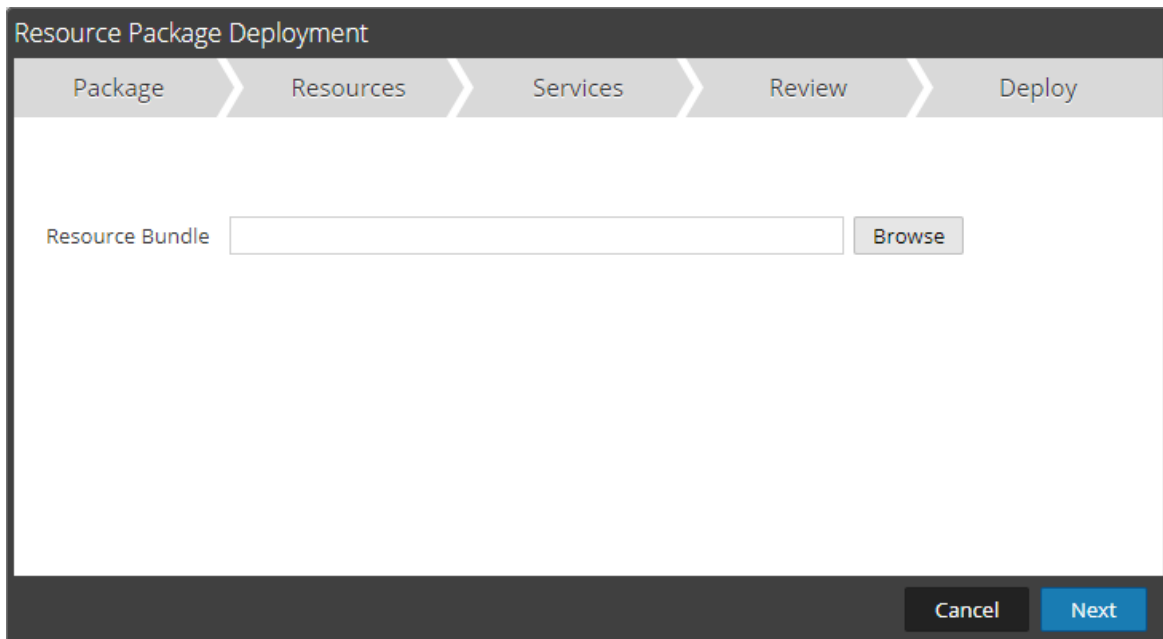
1. Go to  (Configure) > Live Content.
2. Select a group of resources, or a previously created resource package.  
To select a resource or group of resources:
  - a. In the **Live Search View**, browse Live resources (for example, search for the **Log Collector** resource Type).
  - b. In the **Matching Resources** panel, select **Show Results > Grid**.
  - c. Select the checkbox to the left of the resources that you want to deploy.



d. In the Matching Resources toolbar, click Deploy .




3. To select a resource package to deploy:
  - a. In the **Live Search** view - **Matching Resources** toolbar, select **Package** > **Deploy** .  
The Package page of the Resource Package Deployment wizard is displayed.




- b. Click **Browse** and select a package from your network (for example **resourceBundle-FeedsParsersContent.zip**).
- c. Click **Open**.

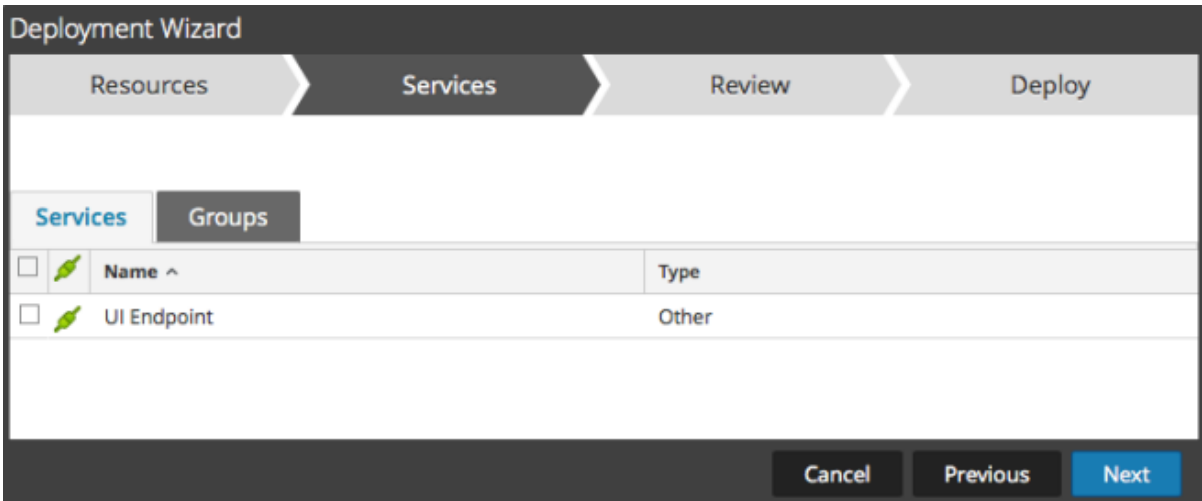
At this point, whether you are deploying a package or a group of resources, the **Deployment Wizard** opens, and the **Resources** page is displayed.

4. Click **Next**.

The **Services** page displayed has two tabs, **Services** and **Groups**, which provide a list of services and service groups that are configured in the  (**Admin**) > **Services** view. The columns are a subset of the columns available in the Services view.

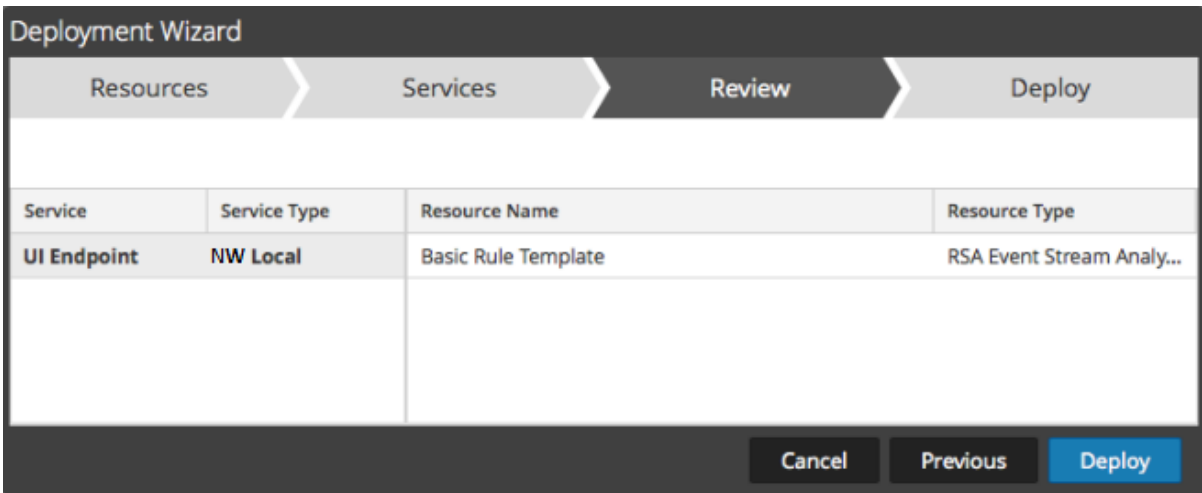
**Note:** The Live server is "smart" about deploying resources to Services. For example, it does not deploy resources that have a Medium of packets to any Log Decoders. This means that only applicable content resources are deployed to each Service.

5. Select the services on which you want to deploy the content. You can select any combination of services and service groups.
  - Use the **Services** tab to select individual services, list of services, and service groups that are configured in the  (**Admin**) > **Services** view.
  - Use the **Groups** tab to select groups of services.



6. Click **Next**.

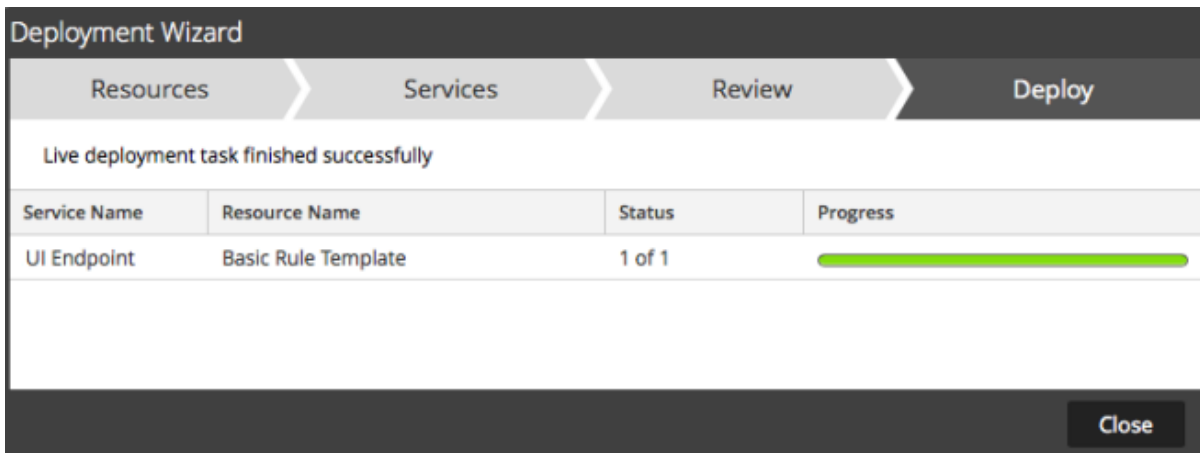
The **Review** page is displayed.



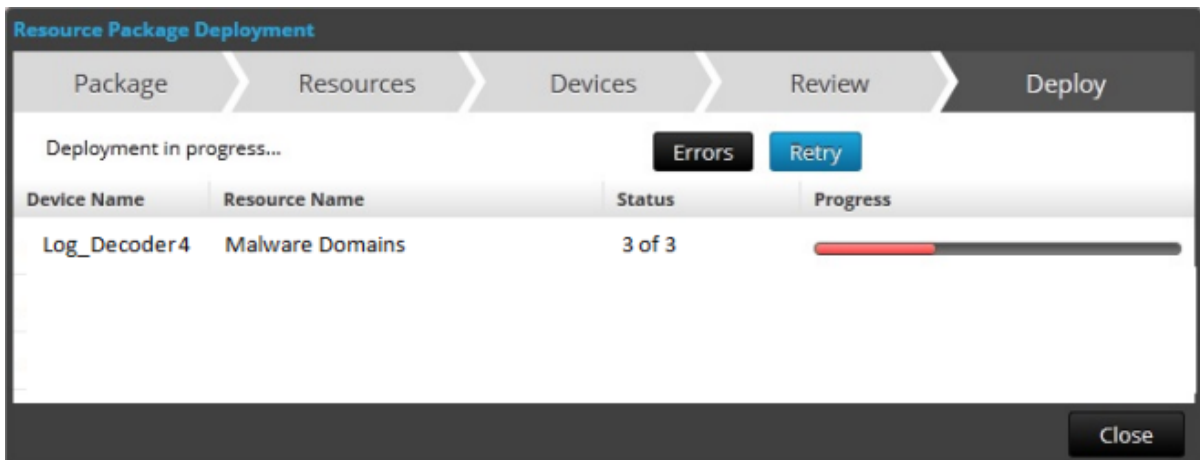
Make sure that you have selected correct resources and the services on which you want to deploy them.

7. Click **Deploy**.

The **Deploy** page is displayed. The Progress bar turns green when you have successfully deployed the resources to the selected services.



If you try to deploy resources and services that are not compatible, NetWitness displays the Errors and Retry buttons, which you can click to review the errors and re-attempt the deployment.




8. Click **Close**.

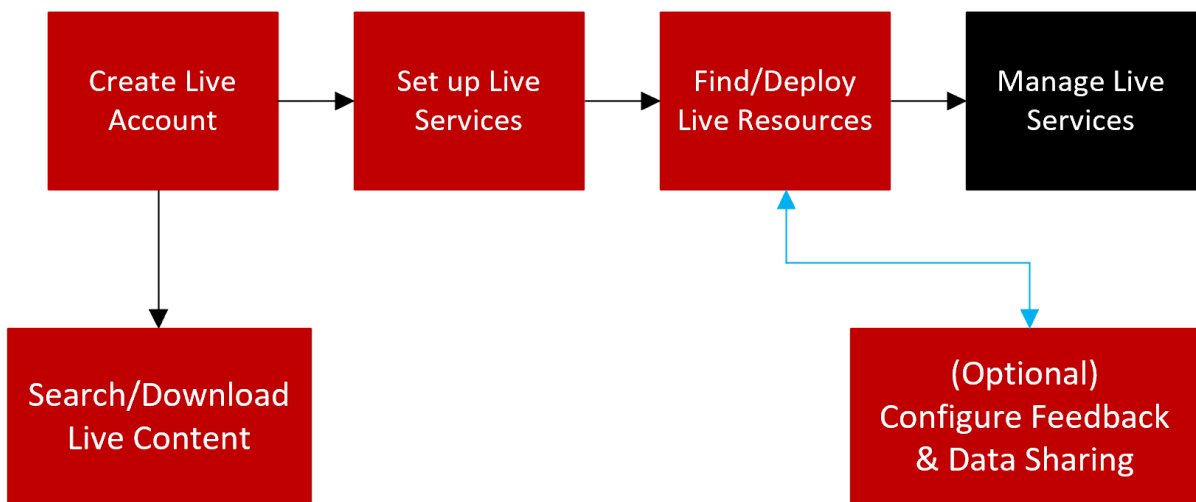
### Next steps

After deploying parsers to Decoders and Log Decoders, you must enable parsers on the individual services. For more information, see the *Decoder and Log Decoder Configuration Guide*.



## Manage Live Resources


With a connection to the CMS server, you can search for, subscribe to, and deploy resources from Live in accordance with your subscription level. Once you have found resources, you deploy them to services and service groups that have been configured in the the  (Admin) > Services view.



There are several workflows for deploying resources to services and managing those deployments. These include:

- Subscribe and deploy resources
- Deploy a resource bundle
- Remove deployments of resources
- Download resources
- Set up data feeds








## Manage Subscription and Deployment

The subscription and deployment workflow takes advantage of the resource management tools available in Live. By subscribing to resources, you agree to receive updated resources in accordance with the synchronization configured in the  (Admin) > System > Live Services panel.

By adding subscribed resources to the deployments list, you configure NetWitness to automatically push those resources to the selected services at the configured synchronization intervals. This method requires some planning of service groups and services where resources are deployed. In addition:

- You can remove a resource from the deployments list in the [Deployments Tab](#).
- You can unsubscribe from a resource in the [Subscriptions Tab](#) and the [Live Resource View](#).

### To manage subscriptions and deployment:

1. In the  (**Admin**) > **System** > **Live Services** panel, specify an interval at which NetWitness checks for updates to subscribed resources in Live and specify the email addresses of people to receive an email listing subscribed resources that have been updated.
2. In the  (**Configure**) > **Live Content** search view, search for and subscribe to Live resources.
3. In the  (**Configure**) > **Subscriptions** > **Deployments** tab, select subscribed resources and add them to the deployment list for services groups.
4. (Optional) In the  (**Configure**) > **Subscriptions** > **Deployments** tab, click  to deploy the resources listed in the Deployments tab immediately.
5. In the  (**Configure**) > **Subscriptions** > **Deployments** tab, select deployed resources from a Group, and remove them from services.
6. In the  (**Configure**) > **Subscriptions** tab, unsubscribe from resources.

### Remove a Deployed Resource

Once deployed to a service, Live resources remain on the service until removed. It is a good practice to remove unused resources from services on which they are deployed.

### To remove deployed resources:

1. Go to the [Live Resource View](#)
2. Unsubscribe from a resource, and remove it from deployed services.

### Deploy a Resource Bundle

To deploy a content package, use the [Resource Package Deployment Wizard](#). You can deploy a content package created in Live to one or more services. NetWitness accepts packages in **.nwp** files or **.zip** files.


### Download Resources

To download resources to your local file system, use the **Download** button in the Live Resource view.

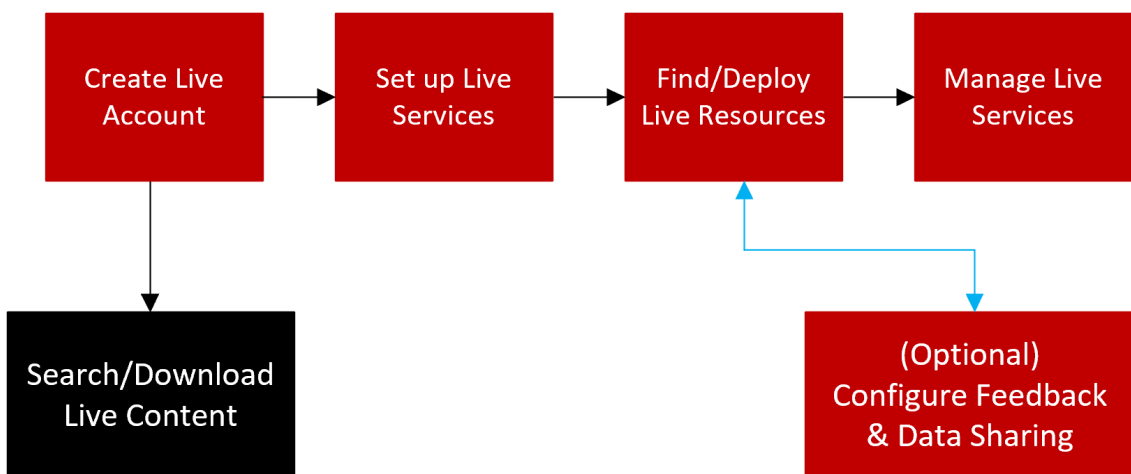
### Set Up Data Feeds

In the **Live** > **Feeds** view, you can set up and maintain Custom and Identify feeds.

## Search and Download Content from NetWitness XDR Cloud Services Live

Administrators can search for live content using the Search Content panel in the NetWitness XDR Cloud Services Live, which is similar to browsing the live CMS content in the  (Configure) > Live Content page on the NetWitness Platform XDR.

**Note:** If Admin server is not connected to the Live Services, you can use the NetWitness XDR Cloud Services Live to search and download the required content.



### Prerequisites

- Ensure that you have created the Live account. For more information, see [Create Live Account](#).

### Quick Search for Content

You can now select and view the content based on the Sources available in the Cloud Services Live. You can select either NetWitness or Community from the Source drop-down list.

- **NetWitness:** Displays all the content provided by NetWitness.
- **Community:** Displays the content collected and retrieved from third party and open source communities.

**Note:** The **Only Opensource** option will appear under the Search Content panel only when the community is selected as the source. You can use this option to select and search open-source related content.

You can also quickly select and view the available content types under Content section.


Clicking  expands the **Content** section and displays the following options:

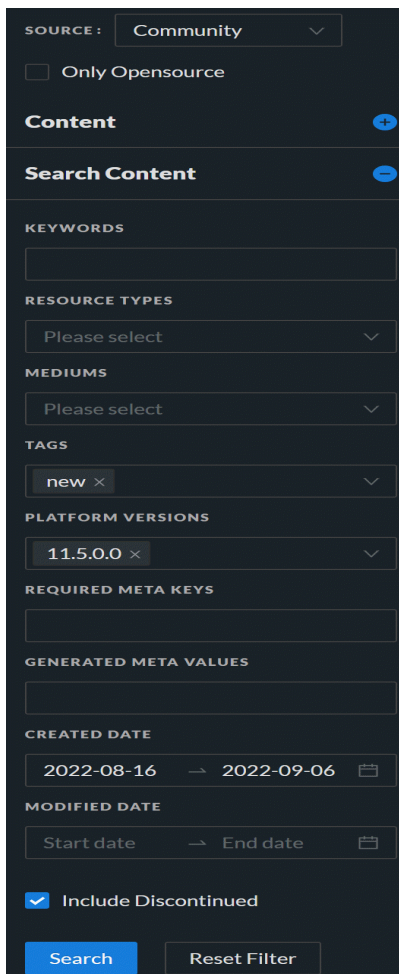
- **New:** Displays the content which is created in the last 21 days.
- **Recently Updated:** Displays the content which is created or updated in the last 21 days.

## Advanced Search for Content

You can search for the specific content in the Search Content view. For more information, see [Live Search Content View](#).

### To search the content:

1. Click  to expand the **Search Content** section.
2. In the **Search Content**, specify the search criteria. Enter any or all of these: keyword, type of resource, medium, tag, platform versions, meta keys, meta values, date when content was created, date when content was modified, and (optional) discontinued content.



The screenshot shows a dark-themed search filter panel. At the top, there is a 'SOURCE' dropdown menu set to 'Community'. Below it is an unchecked checkbox for 'Only Opensource'. The 'Content' section is expanded, showing a '+' icon. The 'Search Content' section is collapsed, showing a '-' icon. The filter criteria are as follows: 'KEYWORDS' is an empty text input; 'RESOURCE TYPES' is a dropdown menu with 'Please select'; 'MEDIUMS' is a dropdown menu with 'Please select'; 'TAGS' has a 'new' tag with a close button; 'PLATFORM VERSIONS' has a '11.5.0.0' tag with a close button; 'REQUIRED META KEYS' is an empty text input; 'GENERATED META VALUES' is an empty text input; 'CREATED DATE' is a date range from '2022-08-16' to '2022-09-06'; 'MODIFIED DATE' is a date range with 'Start date' and 'End date' labels; and 'Include Discontinued' is a checked checkbox. At the bottom, there are 'Search' and 'Reset Filter' buttons.

3. Click **Search**.  
The matching results are displayed on the right panel.

**Content**  
View New, recently updated and community content details here.

Showing **Filtered Content (877)** Timezone: GMT+0530 Asia/Calcutta

NAME ↓	CREATED ↓	UPDATED ↓	TYPE ↓	MIN PLATFORM VERSION ↓	DESCRIPTION ↓	DISCONTINUED ↓
<a href="#">RSA OSINT IP Threat Intel...</a>	11-Sep-2020 01:2...	17-Jul-2022 10:01...	Feed	All Versions	This feed contains IP Address (IPv4 and IPv6) indicators that a...	No
<a href="#">Logs Dashboard</a>	26-Nov-2020 16:5...	26-Nov-2020 16:5...	Not found	11.5.0.0	This dashboard provides information on various NetWitness P...	No
<a href="#">Packet Overview Dashboard</a>	26-Nov-2020 16:5...	26-Nov-2020 16:5...	Not found	11.5.0.0	This dashboard provides information on NetWitness Platform ...	No
<a href="#">RSA OSINT Non-IP Threat L...</a>	11-Sep-2020 01:2...	17-Jul-2022 10:01...	Feed	All Versions	This feed contains Non-IP Address, text based indicators like ...	No
<a href="#">Endpoint Server to Agent ...</a>	26-Nov-2020 16:3...	26-Nov-2020 16:3...	Not found	11.5.0.0	Amount of Incoming UDP Packets Requested by Endpoint ser...	No
<a href="#">Decoder Capture Not Start...</a>	26-Nov-2020 16:4...	26-Nov-2020 16:4...	Not found	11.5.0.0	Capture is not started on this Decoder service, so packet data ...	No
<a href="#">Debian Package Hash Mis...</a>	06-Aug-2020 20:5...	13-Aug-2020 00:4...	Application Rule	11.5.0.0	A hash mismatch may indicate a file has been altered from its o...	No
<a href="#">AWS Route53 Resolver</a>	23-Dec-2020 16:4...	23-Dec-2020 16:4...	Log Device	11.5.0.0	Log device content for event source AWS Route53 Resolver - ...	No
<a href="#">Cisco Umbrella</a>	19-Mar-2021 19:3...	19-Mar-2021 19:3...	Log Device	11.5.0.0	Log device content for event source Cisco Umbrella - cisco_um...	No
<a href="#">Reporting Engine Available ...</a>	26-Nov-2020 16:2...	26-Nov-2020 16:2...	Not found	11.5.0.0	Reporting Engine home directory /var/netwitness/re-server/r...	No
<a href="#">Contexthub Server Query ...</a>	26-Nov-2020 16:4...	26-Nov-2020 16:4...	Not found	11.5.0.0	80% of the Contexthub Server's query response cache is in use.	No
<a href="#">Decoder Capture Rate Zero</a>	26-Nov-2020 16:3...	26-Nov-2020 16:3...	Not found	11.5.0.0	Decoder is presently not capturing data.	No

You can sort the content using the name, created, updated, type, or any of the column.

**Note:** Clicking **Reset Filter** removes the existing filters applied from the **Search Content**, and displays all the available content on the right panel.

## Download Content

You can download the content from the results displayed in NetWitness XDR Cloud Services and upload it to NetWitness Platform XDR Live. The content is downloaded as a package (tar.gz file) that contains tag metadata, medium metadata, contents metadata, and raw contents.

For more information, see [Quick Search for Content](#).

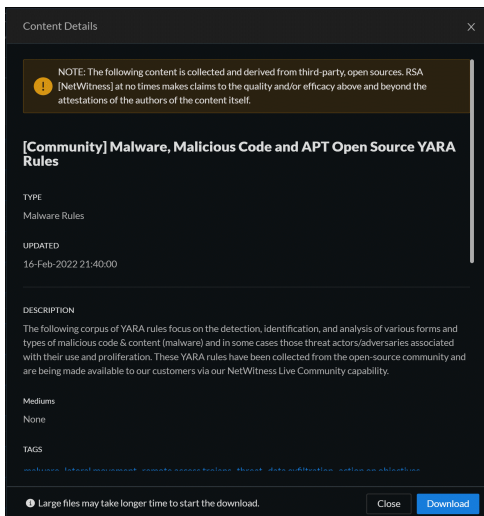
**Note:**

- NetWitness provides no assurance related to the quality and accuracy of the content provided by the third parties and open source communities.

### To download the raw content:

1. Click the name of the content that you want to download.

The **Content Details** dialog is displayed.



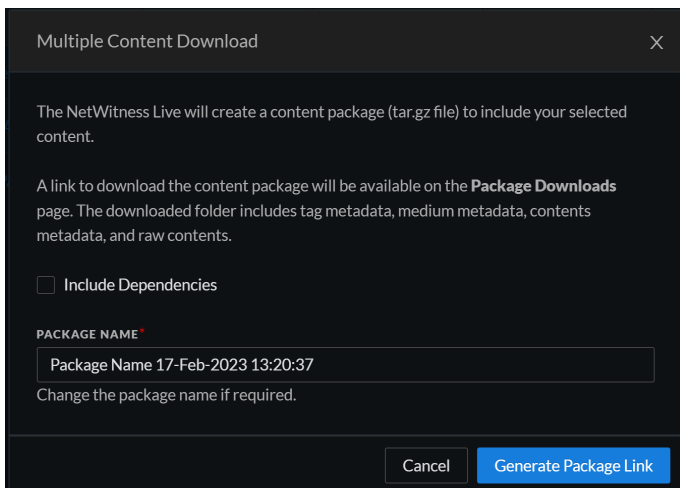
2. Click **Download**.


The content file is downloaded.

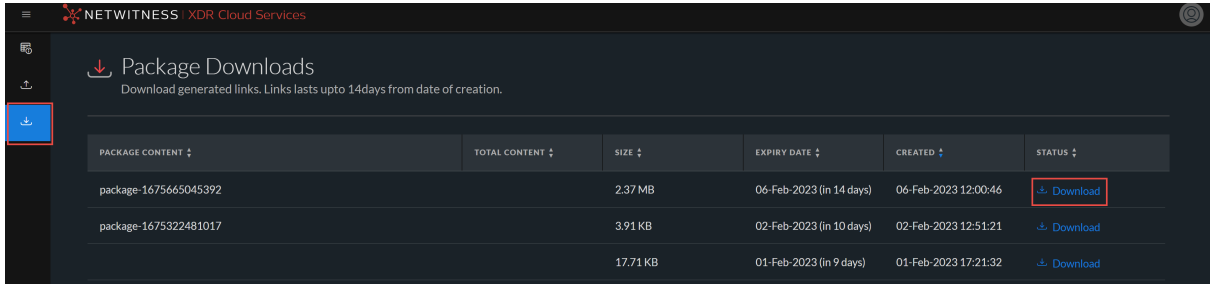
**To download the one or more content:**

1. Log in to the NetWitness XDR Cloud Services using your Live account credentials.  
URL: <https://live.netwitness.com/registration>.
2. Select one or more content you want to download and click **Generate Content Package**.  
A **Multiple Content Download** dialog is displayed.
3. If required, select the **Include Dependencies** checkbox to include dependencies for the selected content. You can change the default package name as required.
4. Click **Generate Package Link**.

NetWitness XDR Cloud Services begins the content package (tar.gz file) creation.



5. Go to the  (Package Downloads) page and click **Download** to download the respective package.



PACKAGE CONTENT ↓	TOTAL CONTENT ↓	SIZE ↓	EXPIRY DATE ↓	CREATED ↓	STATUS ↓
package-1675665045392		2.37 MB	06-Feb-2023 (in 14 days)	06-Feb-2023 12:00:46	<a href="#">Download</a>
package-1675322481017		3.91 KB	02-Feb-2023 (in 10 days)	02-Feb-2023 12:51:21	<a href="#">Download</a>
		17.71 KB	01-Feb-2023 (in 9 days)	01-Feb-2023 17:21:32	<a href="#">Download</a>

The downloaded folder includes tag metadata, medium metadata, contents metadata, and raw contents. You must extract (unzip) the content package, select each of the raw content files and upload it to the appropriate devices or services on NetWitness Platform XDR.

## Additional Procedures

This topic explains the additional procedures an administrator could choose to follow which are not essential for the configuration or use of Live Services.

- [Export Data to RSA](#)
- [Packaging Resources](#)
- [Manage Custom Feeds](#)
  - [Creating a Custom Feed](#)
  - [Create a STIX Custom Feed](#)
  - [Creating and Managing an Identity Feed](#)
  - [Editing a Feed](#)
  - [Removing a Feed](#)
- [Miscellaneous Live Services Procedures](#)



## Export Data to RSA

A NetWitness administrator can export the metrics in NetWitness for Live Feedback.

### About Live Feedback

In the Live Services Configuration panel, there is a Live Feedback Activity Log which enables you to download the usage data required for Live Feedback. This is active regardless of the Live Account configuration.

If the Live Account is not configured, you can manually upload the usage data to RSA. For more information, see the "Configure Live Services Panel" topic in the *System Configuration Guide*.

You must first download the Live Feedback historical data, and then upload it to share with RSA.

### Download Live Feedback Historical Data

To download the Live Feedback historical data:

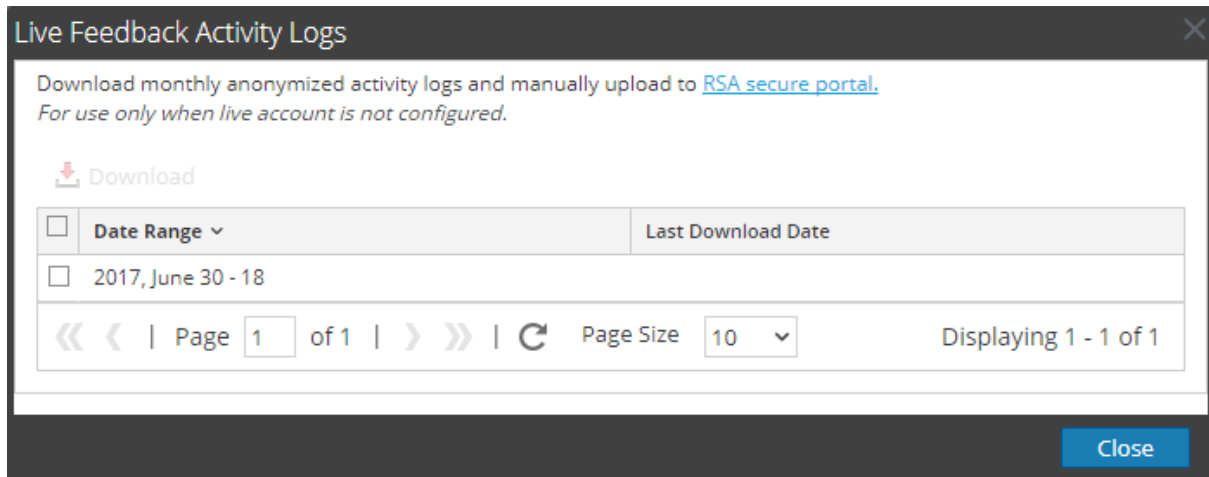
1. Go to  (Admin) > System.

2. In the options panel, select **Live Services**.

The **Live Account** screen is displayed which consists of the **RSA Live Status** and **Download Live Feedback Activity Log**.

3. Click **Live Feedback Activity Log**.

The **Live Feedback Activity Log** window opens which allows you to download the required Live Feedback historical data.



4. Select one or multiple entries by selecting the checkboxes and click **Download**.

**Note:** If you select multiple entries in the history table, the Live Feedback data is downloaded into a ZIP archive, consisting of individual JSON files for each month.


### Share Telemetry Data to NetWitness

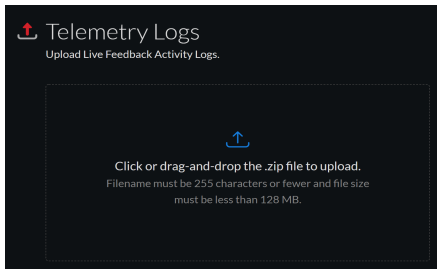
After you download the Live Feedback data, you can then upload it using the following procedure.

**Note:**

- To download the Live Feedback data, see topic [Download Live Feedback Historical Data](#).
- You can share data through NetWitness XDR Cloud Services Live portal. For more information, [Create Live Account](#).

**To share the data to NetWitness**

1. Log in to the NetWitness XDR Cloud Services using your Live account credentials.
2. Click  on the left panel.  
The **Telemetry Logs** dialog is displayed.



**Note:**

- You can upload only .zip files.
- Filename must be 255 characters or less and file size must be less than 128 MB.

3. Click or drag-and-drop a file onto this area to upload.

## Packaging Resources

The primary use for creating and subsequently deploying a resource package is for customers using an air gap network environment. In this case, you create a resource package on the network that is connected to the internet, and then deploy the resource package on a more secure network.

### Create and Deploy Resource Package Use Case

The basic steps are as follows:

1. Access NetWitness Live Services using an instance that is connected to the internet.
2. Create a Resource package as described below, adding whichever content items you need.
3. Copy the ZIP archive of the packages to your secure NetWitness instance, by using a thumb drive or other manual copying process.
4. On the secure NetWitness instance, deploy the resource package. For more information, see [Resource Package Deployment Wizard](#).


### Prerequisites to Create a Resource Package

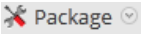
A prerequisite for creating resource packages is configuration of the connection and synchronization between the CMS server and NetWitness and the ability to search for resources in the User Interface.

### Creating a Resource Package

The following procedure describes how to create a resource package, as a ZIP archive and save it to your local file system.

#### **To create a resource package:**


1. Go to  **(Configure)** > **Live Content** from the NetWitness UI.
2. Select the resources that you want to package in the Matching Resources grid.

3. Select some or all the resources that are listed in the Matches Resources pane.
4. Select  **Package** > **Create**.

NetWitness creates a **.zip** archive that contains the selected resources and downloads it to your default download folder. NetWitness gives the package a generic name. You should rename it when you save it so that it identifies the resources contained in the package.

## Creating Threat Package

The following procedure describes how to create a resource package that contains all the content that is categorized as **Threat**. Then we rename it, using the type of content and date.

1. Go to  **(Configure)** > **Live Content**.
2. From the **Category** section, select **Threat**.
3. Select all items returned by clicking on the checkbox in the column header row of the **Matching Resources** pane.

Search Criteria

Keywords

Category

- FEATURED
- THREAT**
  - Attack Phase
  - Malware
- IDENTITY
- ASSURANCE
- OPERATIONS
- SPECTRUM
- MALWARE ANALYSIS

Resource Types

Medium

Search

Matching Resources

Show Results | Details | Deploy | Subscribe | Package

Name	Created	Updated	Type	Description
Local or Guest User Acco...	2022-05-27 11:28 AM	2022-05-27 11:28 AM	Application Rule	This rule triggers when a Local or Guest user...
Clears Application Event ...	2021-10-11 2:41 PM	2021-10-11 2:41 PM	Application Rule	Tampering with windows event logging car...
Deletes Shadow Volume ...	2021-10-11 2:40 PM	2021-10-11 2:40 PM	Application Rule	Deleting shadow volume copies can be an i...
Runs Regsvcs or Regasm	2022-03-08 1:40 PM	2022-03-08 1:40 PM	Application Rule	Regsvcs and Regasm are digitally signed W...
Enumerates Network Co...	2022-06-02 8:11 AM	2022-06-02 8:11 AM	Application Rule	Enumeration of network connections can I...
Potential Abuse of Net Ut...	2022-06-02 8:12 AM	2022-06-02 8:12 AM	Application Rule	Net has a great deal of functionality, much...
Follina Command Executi...	2022-08-16 11:18 AM	2022-08-16 11:18 AM	Application Rule	This rule looks for command line argumen...
Suspicious MSDT Parent P...	2022-08-16 7:04 PM	2022-08-16 7:04 PM	Application Rule	During exploitation of CVE-2022-30190 (Foll...
Changes to GPO or Group...	2022-07-28 7:54 AM	2022-07-28 7:54 AM	Application Rule	This rule detects when any changes are m...
Disables Windows Defend...	2019-04-10 2:15 PM	2021-10-11 2:37 PM	Application Rule	Disabling windows defender using powersl...
Domain User Account Cre...	2022-05-27 11:29 AM	2022-05-27 11:29 AM	Application Rule	This rule detects when a new domain user...
Possible Impacket Host A...	2022-03-29 7:37 PM	2022-06-21 6:19 PM	Application Rule	Detect possible Impacket psexec usage on...
Potential Abuse of COM ...	2022-06-09 4:49 PM	2022-06-09 4:49 PM	Application Rule	Adversaries may establish persistence by c...
[Community] Possible Qa...	2022-03-24 5:19 PM	2022-06-29 1:54 PM	Application Rule	Once on a victim host, Qakbot performs se...
[Community] Nerbian RA...	2022-06-30 1:34 PM	2022-06-30 1:34 PM	Application Rule	Following rule helps to detect known techn...
Unexpected fodhelper.ex...	2022-08-25 11:15 AM	2022-08-25 11:15 AM	Application Rule	fodhelper (Features On Demand Helper) is...

320 Matching Resources

4. Select **Package** > **Create**.

A ZIP archive is saved to your Downloads folder. For example, **resourceBundle8740753704980701969.zip**.

5. Rename the package to something meaningful. For example, in this case, you could change the package name to **threatResourceBundle\_2018\_01\_31.zip** (assuming today's date is January 31, 2018).

The resource package is now available for later deployment.

### Deploying a Threat Package

This procedure assumes that you saved a package named **threatResourceBundle\_2018\_01\_31.zip**, as described in the previous section. It describes how to deploy a saved resource package

1. Go to **(Configure)** > **Live Content**.
2. In the **Matching Resources** pane, select **Package** > **Deploy**.
3. Click **Browse** and navigate to the **threatResourceBundle\_2018\_01\_31.zip** file that were created earlier.

Resource Package Deployment

Package > Resources > Services > Review > Deploy


Resource Bundle: threatResourceBundle\_2018\_01\_31.zip **Browse**

**Cancel** **Next**

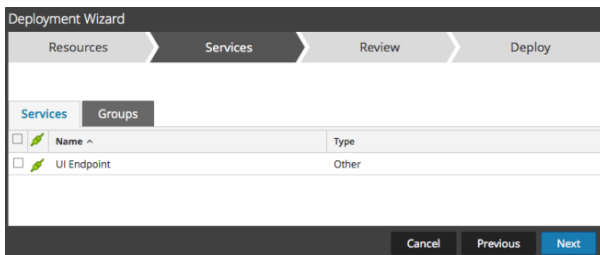
4. Click **Next**.

The **Resources** page displays details for the resources in the package.

5. Click **Next**.

The **Services** page displays two tabs, **Services** and **Groups**, which provide a list of services and service groups that are configured in the  (**Admin**) > **Services** view. The columns are a subset of the columns available in the Services view.

6. Select the services on which you want to deploy the content. You can select any combination of services and service groups.



7. Click **Next**.

The **Review** page is displayed.

**Note:** Make sure that you have selected correct resources and the services to which you want to deploy them.

8. Click **Deploy** to complete the deployment process. Alternatively, you can choose **Cancel** or **Previous** to either cancel the deployment or go back to the previous screen.

## Manage Custom Feeds

The custom feed capability is implemented using the Custom Feed Wizard in NetWitness, allowing you to quickly populate Decoders with custom and identity feeds.

### Custom Feed Creation

You can use the **Live > Custom Feeds > Setup Feed > Configure a Custom Feed** wizard to create and deploy Decoder feeds based on deterministic logic that offers the meta keys specific to the selected Decoders and Log Decoders. Although the wizard guides you through the process to create both on-demand and recurring feeds, you should understand the form and content of a feed file when you create a feed.

Feed file names in NetWitness are in the form `<filename>.feed`. To create a feed, NetWitness requires a feed **data** file in `.csv` or `.xml` (for STIX) format and a feed **definition** file in `.xml` format, which describes the structure of a feed data file. The Configure a Custom Feed wizard can create the feed definition file based on a feed data file, or based on a feed data file and the corresponding feed definition file.

The files that you use to create an on-demand feed must be stored on your local file system. The files used to create a recurring feed must be stored at an accessible URL, whence NetWitness can fetch the most current version of the file for each recurrence. After a NetWitness feed is created, you can download the feed to your local file system, edit the feed files, and edit the NetWitness feed to use the updated feed files.

### Sample Feed Definition File

This is an example of a feed definition file named `dynamic_dns.xml`, which NetWitness creates based on your entries in the Feed wizards. It defines the structure of the feed data file named `dynamic_dns.csv`.

**Note:** The feed file path should be `.csv` regardless of the Feed Type (Default or STIX).

#### Sample Feed Definition File

```
<?xml version="1.0" encoding="utf-8"?>
<FDF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">
  <FlatFileFeed name="Dynamic DNS Domain Feed"
    path="dynamic_dns.csv"
    separator=","
    comment="#"
    version="1">

    <MetaCallback
      name="alias.host"
      valuetype="Text"
      apptype="0"
      truncdomain="true"/>

    <LanguageKeys>
      <LanguageKey name="threat.source" valuetype="Text" />
    </LanguageKeys>
  </FlatFileFeed>
</FDF>
```

```

    <LanguageKey name="threat.category" valuetype="Text" />
    <LanguageKey name="threat.desc" valuetype="Text" />
  </LanguageKeys>

  <Fields>
    <Field index="1" type="index" key="alias.host" />
    <Field index="4" type="value" key="threat.desc" />
    <Field index="2" type="value" key="threat.source" />
    <Field index="3" type="value" key="threat.category" />
  </Fields>

</FlatFileFeed>
</FDF>

```

### Feed Definition Equivalents for Custom Feed Wizard Parameters

The NetWitness Feeds wizard provide options to define the structure of the data feed file. These correspond directly to attributes in the feed definition (.xml) file.

NetWitness Parameter	Feed Definition File Equivalent
<b>Define Feed</b> tab	
<b>Feed Type</b>	Select: <b>Default</b> - to define a feed based on a .csv formatted feed data file. <b>STIX</b> - to define a feed based on STIX formatted .xml file.
<b>Feed Task Type</b>	Select: <b>Adhoc</b> - to create an on-demand feed. <b>Recurring</b> - to create a feed that recurs automatically.
<b>Name</b>	Enter a custom feed name in the feed data file that corresponds to the flatfeedfile name attribute in the feed definition file; for example, Dynamic DNS Test Feed.
<b>File/ Browse</b>	Enter a name of the feed data file that corresponds to the flatfeedfile path attribute in the feed definition file; for example, dynamic_dns.csv.
(STIX, Recurring) <b>Trust All Certificate</b>	Select <b>Trust All Certificate</b> , if you do not want to validate the REST server certificate. This option is enabled by default (checked).
(STIX, Recurring) <b>Certificate/Browse</b>	For client authentication with the REST URL, in the <b>Certificate</b> field, click <b>Browse</b> and select the self signed certificate. The supported certificate formats are .cer, .crt with Base64 & DER encoded files.
<b>Define Feed</b> tab - Advanced Options	
<b>XML Feed File</b>	Enter a name of the feed definition file, for example, dynamic_dns.xml.
<b>Separator</b>	The separator character used to separate attributes in the feed data file. It corresponds to the flatfeedfile separator in the feed definition file; for example, a comma.



NetWitness Parameter	Feed Definition File Equivalent
<b>Comment</b>	The character used to identify a comment in the feed data file. It corresponds to the <b>flatfeedfile comment</b> attribute in the feed definition file; for example, #.
<b>Remove STIX data older than</b>	The number of days for which the STIX packages downloaded from TAXII server have to be stored. The STIX packages older than the specified number of days are deleted automatically. The default value is 180 days, which is also the maximum.
<b>Select Services tab</b>  (Define Columns tab, Define Index) <b>Type</b>	Select the services to which you want to send the data feed.  The type of lookup value in the index position of the feed data file. <b>IP</b> means that each row in the feed data file contains an IP address in the lookup value position. The IP value is in dotted-decimal format (for example, 10.5.187.42). <b>IP Range</b> means that each row in the feed data file contains a range of IP addresses in the lookup value position. The IP range is in CIDR format (for example, 192.168.2.0/24). <b>Non IP</b> means that the each row in the feed data file contains a metadata value other than IP address in the lookup value position. The Service Type and Truncate Domain, and Callback Keys fields become active for a Non IP index.
(Define Columns tab, Define Index) <b>CIDR</b>	Specifies that the IP value in the lookup position is in CIDR format. The <b>CIDR</b> attribute sets the IP address format in the field to Classless Inter-Domain Routing (CIDR) notation.
(Define Columns tab, Define Index) <b>Service Type</b>	For a Non IP index, the integer service type to filter meta lookups. It corresponds to <b>MetaCallback apptype</b> attribute in the feed definition file. A value of <b>0</b> indicates no filtering by service type.
(Define Columns tab, Define Index) <b>Truncate Domain</b>	For a Non IP index, for meta values that contain domain names (for example, hostnames), the system can strip off the host specific element in the data. Truncate Domain corresponds to the <b>MetaCallback truncdomain</b> attribute. If the value is www.example.com, it is truncated to example.com. A value of <b>False</b> selects no truncation, and <b>True</b> selects truncation.
(Define Columns tab, Define Index) <b>Ignore Case</b>	If this option checked, the feed will ignore the case.
(Define Columns tab, Define Index) <b>Callback Keys</b>	For a Non IP index, the available meta keys to match on instead of ip.src/ip.dst (the defaults for IP index type) are selectable from the drop-down list. The Callback Key corresponds to the <b>MetaCallback name</b> attribute, and the index column of the csv file must contain data that can match the chosen meta key. For example, if the username meta key is chosen, the index column of the csv file needs to be populated with users to be matched.

NetWitness Parameter	Feed Definition File Equivalent
(Define Columns tab, Define Index) <b>Index Column</b>	Identifies the column in the feed data file that provides the lookup value for the row. Each position in each row of the feed data file is identified by a <b>Field index</b> attribute in the feed definition file. A field with an index of <b>1</b> is the first entry in a row, the second field has an index of <b>2</b> , the third field has an index of <b>3</b> , and so on. You can select multiple index columns, if the <b>Feed Type</b> is <b>STIX</b> and <b>Index Type</b> is <b>Non IP</b> . When you select multiple index columns the values from all the selected columns are merged in the first index column that you selected.
(DEFINE VALUES) <b>Key</b>	The name of the <b>LanguageKey</b> , as defined in the feed definition file, for which meta is created from this row of the feed data file. It corresponds to the <b>Field key</b> attribute in the feed definition file. A key applies only to a field whose type is set to <b>value</b> . In the feed definition file, there is a list of LanguageKeys from <b>index.xml</b> , or a summary name if Source Name and Destination Name are used. For example, <b>reputation</b> is a summary name for <b>reputation.src</b> and <b>reputation.dst</b> ). This value is referenced by the Field key attribute.

## Creating a Custom Feed

This topic provides instructions for creating a custom feed using a .csv or STIX formatted feed data file in NetWitness. For more information about STIX and creating a STIX custom feed, see [Create a STIX Custom Feed](#).

You can easily create a custom feed using the Custom Feed wizard. To complete this procedure, you need a feed data file in .csv or .xml format. If you also have an associated feed definition file in .xml format, which describes the structure of the feed data file, you can use the feed definition file to create a feed. The Custom Feed wizard can create the feed based on a feed data file, or based on a feed data file and corresponding feed definition file.

After completing this procedure, you will have created a custom feed.

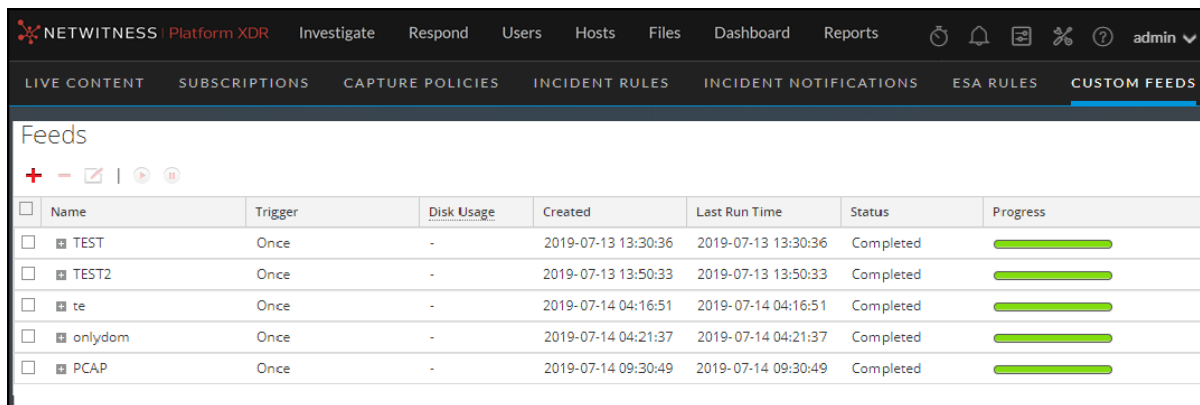
The feed data file (.csv or STIX (.xml)) and optionally the feed definition file (.xml) must be available on the local file system for an on-demand custom feed. For a recurring custom feed, the files must be available at a URL that is accessible to the NetWitness server.

**Note:** Any feeds that are created in 11.2 release or prior will be automatically pushed to Context Hub as Lists. The lists can be looked up in the context lookup panel of the Respond and Investigate pages. If Context Hub is not configured or the service is down, then the feeds will be pushed to Context Hub the next time the server is available.

### To create a custom feed:

1. Go to  (Configure) > CUSTOM FEEDS.

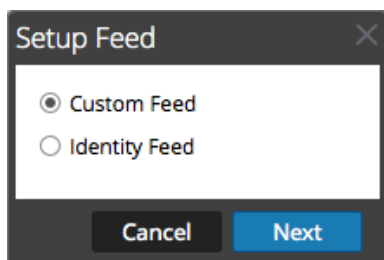
The Custom Feeds view is displayed.



<input type="checkbox"/>	Name	Trigger	Disk Usage	Created	Last Run Time	Status	Progress
<input type="checkbox"/>	TEST	Once	-	2019-07-13 13:30:36	2019-07-13 13:30:36	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>
<input type="checkbox"/>	TEST2	Once	-	2019-07-13 13:50:33	2019-07-13 13:50:33	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>
<input type="checkbox"/>	te	Once	-	2019-07-14 04:16:51	2019-07-14 04:16:51	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>
<input type="checkbox"/>	onlydom	Once	-	2019-07-14 04:21:37	2019-07-14 04:21:37	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>
<input type="checkbox"/>	PCAP	Once	-	2019-07-14 09:30:49	2019-07-14 09:30:49	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>

2. In the toolbar, click .

The Setup Feed dialog is displayed.



**Setup Feed** ✕

Custom Feed

Identity Feed

Cancel
Next

- To select the feed type, click **Custom Feed** and **Next**.

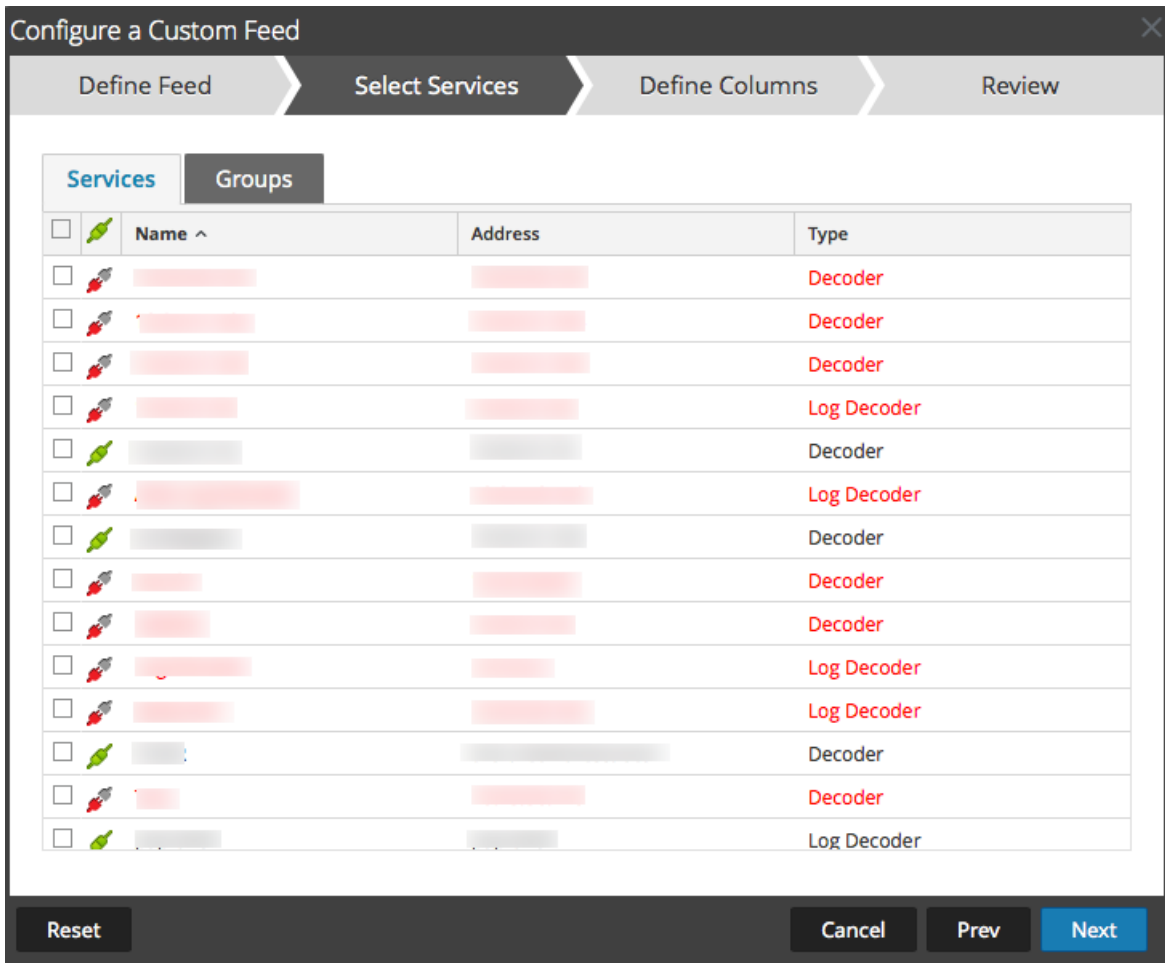
The Configure a Custom Feed wizard is displayed, with the Define Feed form open.

- To define a feed based on a `.csv` formatted feed data file, select **CSV** in the **Feed Type** field.
- To define an on-demand feed task that executes once, select **Adhoc** in the **Feed Task Type** field and do one of the following:
  - (Conditional) To define a feed based on a `.csv` formatted feed data file, type the feed **Name**.
  - Select the checkbox **Upload As CSV File Feed**, if required.
  - Select a `.csv` content **File** from the local file system, and click **Next**.
  - (Conditional) To define a feed based on an XML feed file, select **Advanced Options**.

The Advanced Options are displayed:

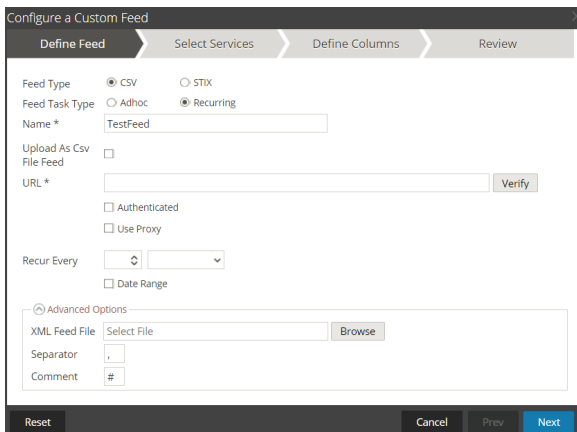
- Select an XML feed file from the local file system, choose the **Separator** (default is comma), and specify the **Comment** characters used in the feed data file (default is #), and click **Next**.
- The Select Services form is displayed. This is an example of the form for a feed based on a feed data file with no feed definition file. If you are defining a feed based on a feed definition file, the

Define Columns tab is not needed.



6. To define a recurring feed task that executes repeatedly at specified intervals, during a specified date range.
  - a. Select **Recurring** in the **Feed Task Type** field.

The Define Feed dialog includes the fields for a recurring feed.



- b. In the **URL** field, enter the URL where the feed data file is located, for example, `http://<hostname>/<feeddatafile>.csv`, and click **Verify**.

NetWitness verifies the location where the file is stored, so that NetWitness can check for the latest file automatically before each recurrence.

- c. (Optional) If the URL has restricted access and requires authentication using your username and password, select **Authenticated**.

NetWitness provides your user name and password for authentication to the URL.

- d. If you want the NetWitness server to access the Feed URL through a proxy, select **Use Proxy**. For more information on configuring a proxy, see the **Configure Proxy for NetWitness** topic in the *System Configuration Guide*. By default, the **Use Proxy** checkbox is not selected.

**NOTE:**

If you are using an HTTPS based feed server, ensure that you import and install the certificates. For more information, see [Import Certificates for HTTPS Service](#)

- e. To define the interval for recurrence, do one of the following:
- Specify the number of minutes, hours, or days between recurrences of the feed.
  - Specify recurrence every week, and select the days of the week.
- f. To define the date range for the execution of the feed to recur, specify the **Start Date** and time and the **End Date** and time.

The screenshot shows the 'Configure a Custom Feed' dialog box with the 'Define Feed' tab selected. The 'Feed Type' is set to 'Default'. The 'Feed Task Type' is set to 'Recurring'. The 'Name' field contains 'TestFeed'. The 'URL' field contains 'https://qasa2.netwitness.local/live/feeds'. The 'Recur Every' field is set to '3' and 'Day(s)'. The 'Advanced Options' section is expanded, showing 'XML Feed File' with a 'Browse' button, 'Separator' set to ',', and 'Comment' set to '#'. The 'Date Range' field is collapsed. At the bottom, there are 'Reset', 'Cancel', 'Prev', and 'Next' buttons.

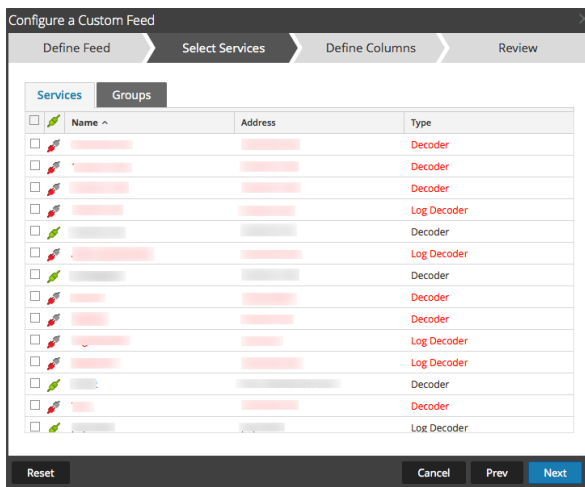
7. (Conditional) If you want to define a feed based on an XML feed file:

- Type the feed **Name**, select **Advanced Options**.

The Advanced Options fields are displayed.

- Select an XML feed file from the local file system, choose the **Separator** (default is comma), specify the **Comment** characters used in the feed data file (default is #) and click **Next**.

The Select Services dialog is displayed.



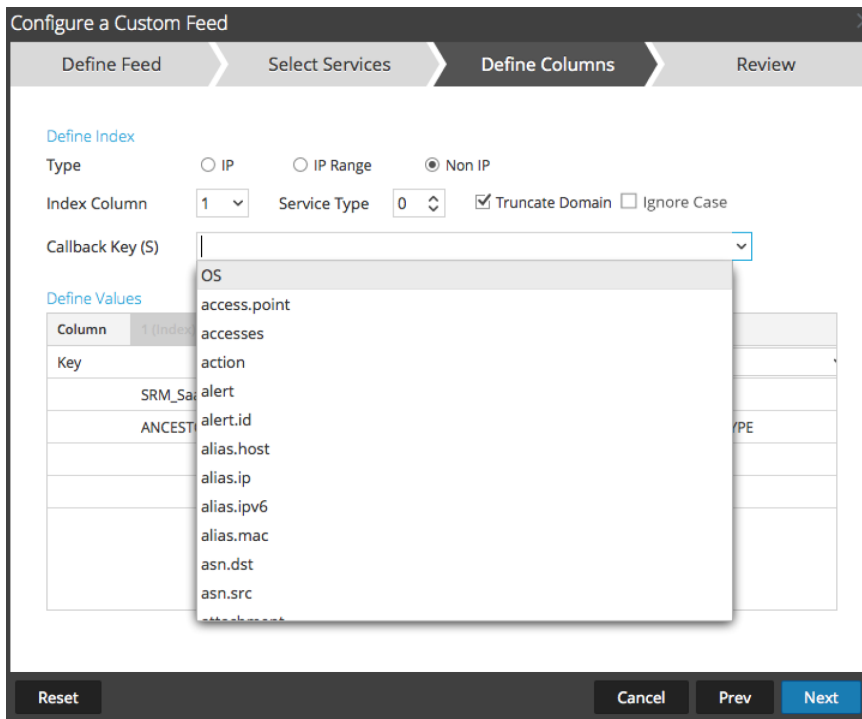
8. To identify services on which to deploy the feed, do one of the following:

- a. Select one or more Decoders and Log Decoders, and click **Next**.
- b. Click the **Groups** tab and select a group. Click **Next**.

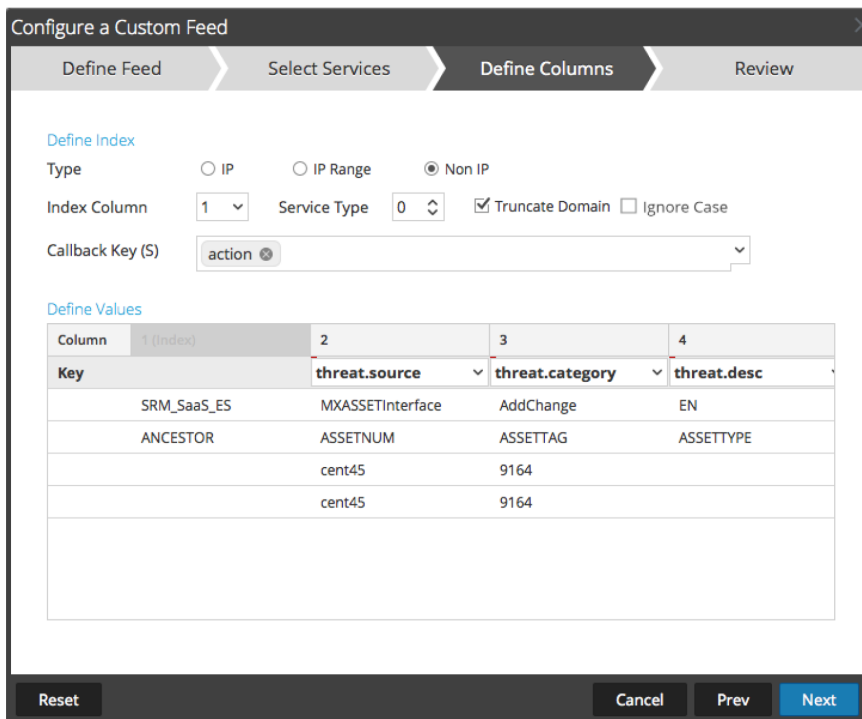
The Define Columns dialog is displayed.

9. To map columns in the Define Columns form:


- a. Define the Index type: **IP**, **IP Range**, or **Non IP**, and select the index column.
- b. (Conditional) If the index type is **IP** or **IP Range** and the IP address is in CIDR notation, select **CIDR**.
- c. (Conditional) If the index type is **Non IP**, additional settings are displayed. Select the service type and **Callback Keys**, and optionally select the **Truncate Domain** and **Ignore Case** option.



- d. Select the language key to apply to the data in each column from the drop-down list. The meta displayed in the drop-down list is based on the meta available for the service define values. You can also add other meta based on advanced expertise.

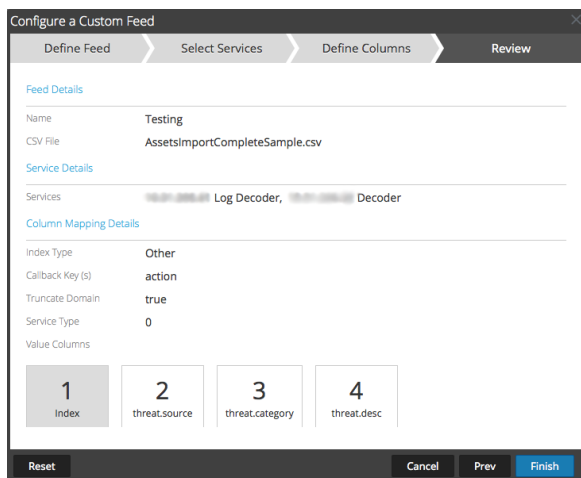




**Note:** When a custom feed gets converted into a context hub list, you must map at least one meta key with one or more meta types by mapping a column header with a meta. However, you can add or edit the entity mapping of a list by clicking  in the Lists tab. For more information, see the *Context Hub Configuration Guide*.

e. Click **Next**.

The Review dialog is displayed.



10. Anytime before you click **Finish**, you can:

- Click **Cancel** to close the wizard without saving your feed definition.
- Click **Reset** to clear the data in the wizard.
- Click **Next** to display the next form (if not viewing the last form).
- Click **Prev** to display the previous form (if not viewing the first form)

11. Review the feed information, and if correct, click **Finish**.

12. Upon successful creation of the feed definition file, the Create Feed wizard closes, and the feed and corresponding token file are listed in the Feed grid and progress bar tracks completion. You can expand or collapse the entry to see how many services are included, and which services were successful.

**Note:** When you create a feed, and if there is no entity mapping done such as in case of custom meta, then those columns in the List will not have entity mappings in Context Hub. You have to manually map the entities from the List page.

### **Import Certificates for HTTPS Service**

Import certificates to communicate with the HTTPS services:

1. SSH to the NW node and copy the CA certificate located in the following directory:  
*/etc/pki/ca-trust/source/*
2. Execute the following command to update the certificates:  
`update-ca-trust`

3. Execute the following command to add the certificate to the java keystore:  
`keytool -list -keystore /etc/pki/java/cacerts -storepass changeit |& head`
4. Restart the service on the NW node.

**Note:** Perform the procedure for all the HTTPS servers.  
Example: HTTPS proxy server and HTTPS feed server.

## Create a STIX Custom Feed

You can create a custom feed using a .csv or STIX formatted feed data file in NetWitness.

**Note:** NetWitness supports Structured Threat Information Expression (STIX) 1.0, 1.1 and 1.2 versions only.

Structured Threat Information Expression (STIX™) is a structured language for describing cyber threat information so it can be shared, stored, and analyzed in a consistent manner. For more information about STIX, see <https://oasis-open.github.io/cti-documentation/>.

**Caution:** If STIX recurring feed is configured and you update Security Analytics from 10.6.x to NetWitness 11.0, you must re-configure the STIX recurring feed.

In NetWitness Platform XDR, STIX feeds are supported. STIX content (with version 11.x) can be uploaded in an ".xml" format. The constructs such as Indicator Title and Description, Observable Title and Description, and Indicator Sightings information are parsed from STIX and pushed to the decoders or log decoders that are selected during feed configuration. Information such as IP addresses, File hashes, Domain names, URIs, and Email addresses are extracted from the STIX observable to be included in the feed.

Make sure the following criteria are met before you upload the STIX file:

1. Only STIX Observables with property values in the "Equals" operator
2. The uploaded STIX xml file must have only one STIX\_Package

TAXII (Trusted Automated eXchange of Indicator Information) is the main transport mechanism for cyber threat information represented in STIX. Using the TAXII services, organizations can share cyber threat information in a secure and automated manner.

The STIX and TAXII communities work closely together to ensure that they continue to provide a full stack for sharing threat intelligence.

Apart from TAXII server, STIX data can also reside on REST server and you can fetch STIX file from the REST server by providing the URL of the REST server. For example, <http://stixrestserver.internal.com>.

The feed data file (.csv or STIX (.xml)) and optionally the feed definition file (.xml) must be available on the local file system for an on-demand custom feed. For a recurring custom feed, the files must be available at a URL that is accessible to the NetWitness server.

In NetWitness Platform XDR, STIX (.xml) feed of type Indicators or Observable which contains the properties such as the IP addresses, File hashes, Domain names, URIs and Email addresses are supported. The properties values in the Equals operator is only supported. The STIX constructs that are parsed are Indicator Title and Description, Observable Title and description and Indicator Sightings information. The STIX (.xml) with a single STIX\_Package is only supported."

### To create a STIX custom feed:

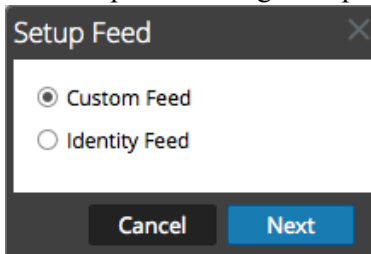
1. Go to  (Configure) > CUSTOM FEEDS.

The Custom Feeds view is displayed.

	Name	Trigger	Disk Usage	Created	Last Run Time	Status	Progress
<input type="checkbox"/>	TEST	Once	-	2019-07-13 13:30:36	2019-07-13 13:30:36	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>
<input type="checkbox"/>	TEST2	Once	-	2019-07-13 13:50:33	2019-07-13 13:50:33	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>
<input type="checkbox"/>	te	Once	-	2019-07-14 04:16:51	2019-07-14 04:16:51	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>
<input type="checkbox"/>	onlydom	Once	-	2019-07-14 04:21:37	2019-07-14 04:21:37	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>
<input type="checkbox"/>	PCAP	Once	-	2019-07-14 09:30:49	2019-07-14 09:30:49	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>

- In the toolbar, click .

The Setup Feed dialog is displayed.



- To select the feed type, click **Custom Feed** and **Next**.

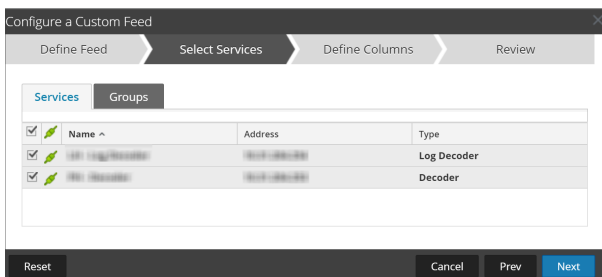
The Configure a Custom Feed wizard is displayed, with the Define Feed dialog open.

- Enter the following details:
  - Feed Type:** Select **STIX**, to define a feed based on a STIX formatted `.xml` file.
  - Name:** type the feed name, to define a feed based on STIX formatted `.xml` file.
  - STIX Source:**Select a STIX data source from the drop-down which is added in Context Hub.
  - Recur Every:** Specify a recurring feed task that executes repeatedly at specified intervals.

**Note:** NetWitness verifies the connection to the server, so that NetWitness can check for the latest file automatically before each recurrence.

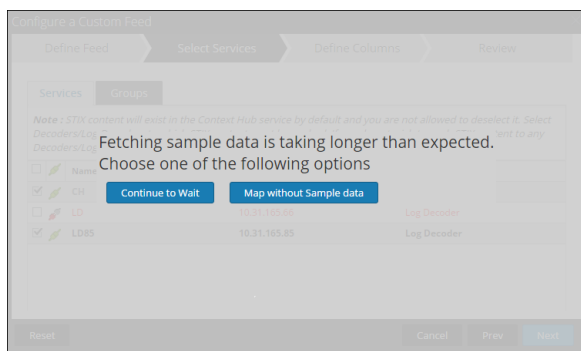
- Date Range:** Select the checkbox and specify the date range for the feed task to recur.

5. (Optional) Select **Advanced Options**, to define a feed based on an XML feed file.
  - a. **XML Feed file:** Browse and select an XML feed file from the local file system.
  - b. **Separator:** Choose a separator (default is comma).
  - c. **Comment:** Specify the comment characters used in the feed data file (default is #).
6. Click **Next**.
7. The Select Services dialog is displayed. This is an example of the form for a feed based on a feed data file with no feed definition file. If you are defining a feed based on a feed definition file, the Define Columns tab is not needed.



8. To identify services on which to deploy the feed, do one of the following:
  - a. Select one or more Decoders and Log Decoders, and click **Next**.
  - b. In case of STIX feed, Context Hub will be selected by default and you are not allowed to deselect it. In addition, you can select one or more Decoders and Log Decoders and click **Next** or Click the **Groups** tab and select a group. Click **Next**.

If the data from the STIX server is large, the following message is displayed:



- If you click **Continue to Wait**, it continues to wait till the sample data is fetched or timeout (10 minutes) whichever is sooner. In case of timeout no sample data is retrieved even after 10 minutes.
- If you click **Map Without Sample data**, the mapping column is displayed without any sample data.

The Define Columns dialog is displayed.

9. To map columns in the Define Columns form:

- a. Define the Index type: **IP**, **IP Range**, or **Non IP**, and select the index column.
- b. (Optional) If the index type is **IP** or **IP Range** and the IP address is in CIDR notation, select **CIDR**.
- c. (Optional) If the index type is **Non IP**, additional settings are displayed. Select the service type and **Callback Keys**, and optionally select the **Truncate Domain** option.

Configure a Custom Feed

Define Feed > Select Services > Define Columns > Review

**Define Index**

Type  IP  Non IP

Index Column(S) 10  CIDR

**Define Values**

Column	1	2	3	4
Key				
Header	Indicator Title	Indicator Description	Observable Title	Observable Description
	Some Indicator	<p>Some Indicator</p>	domain:domain1.exa...	domain:domain1.exa...
	Some Indicator	<p>Some Indicator</p>	domain:domain2.exa...	domain:domain2.exa...
	indicator-domain	auto domain test	domain test	domain desc
	Another Indicator	<p>Another Indicator...	domain:domain3.exa...	domain:domain3.exa...

Reset Cancel Prev Next

**Note:**

- If the **Index Type** is Non IP, you can select multiple index columns in the **Index Column(S)**. The values from all the selected columns are merged in the first index column that you selected and the merged values are pushed to the Log Decoder for parsing. For example, in the **Index Column(S)** if you select 2,4,7 as index columns the values from the 2,4 and 7 columns are merged in the column 2 and the values are pushed to Log Decoder for parsing.
- Indexing cannot be done for the columns such as Indicator Title, Indicator Description, Observable Title, Observable Description, as the look up cannot be performed for those columns.

- d. Select the language key to apply to the data in each column from the drop-down list. The meta displayed in the drop-down list is based on the meta available for the service define values. You can also add other meta based on advanced expertise.
- e. Click **Next**.

The Review dialog is displayed.

**Configure a Custom Feed**

Define Feed > Select Services > Define Columns > **Review**

**Feed Details**

Name: FILESTIX  
XML Feed File: FILESTIX-stix.xml

**Service Details**

Services: PH - Decoder, LH - Log Decoder

**Column Mapping Details**

Index Type: IP  
CIDR: false

Value Columns

10 Index  
24 event.desc

Reset Cancel Prev **Finish**

10. Anytime before you click **Finish**, you can:
  - Click **Cancel** to close the wizard without saving your feed definition.
  - Click **Reset** to clear the data in the wizard.
  - Click **Next** to display the next dialog (if not viewing the last form).
  - Click **Prev** to display the previous dialog (if not viewing the first form)
11. Review the feed information, and if correct, click **Finish**.
12. Upon successful creation of the feed definition file, the Create Feed wizard closes, and the feed and corresponding token file are listed in the Feed grid and progress bar tracks completion. You can expand or collapse the entry to see how many services are included, and which services were successful.

Name	Trigger	Feed Size	Created	Last Run Time	Status	Progress
FILEHASH	Fetches STIX feeds from 2020-May-19 03:16, running every 5 minutes	0 bytes	2020-05-19 03:25:23	2020-05-22 05:16:01	Completed	<div style="width: 100%;"></div>
FILESTIX	Fetches STIX feeds from 2020-May-19 03:32, running every 5 minutes	0 bytes	2020-05-19 03:32:09	2020-05-22 05:12:09	Completed	<div style="width: 100%;"></div>
AllIndicatorsREST	Fetches STIX feeds from 2020-May-19 04:48, running every 5 minutes	0 bytes	2020-05-19 05:03:52	2020-05-22 05:13:26	Completed	<div style="width: 100%;"></div>
ALLIndEdited	Fetches STIX feeds from 2020-May-19 05:13, running every 5 minutes	0 bytes	2020-05-19 05:13:54	2020-05-22 05:13:54	Completed	<div style="width: 100%;"></div>
TAXIIServer1	Fetches STIX feeds from 2020-May-19 05:44, running every 5 minutes	288 bytes	2020-05-19 05:44:38	2020-05-22 05:14:38	Completed	<div style="width: 100%;"></div>

**Note:** Health and Wellness raises alerts when the available heap memory of Context Hub server is critically low and the status displays as unhealthy due to low memory. For more information on how to troubleshoot the `OutOfMemoryError` on the Context Hub Server, see "Troubleshooting" in the *Live Services Management Guide*.

## MetaCallback Feeds using CIDR Index Range for IPv4 and IPv6

You can use CIDR index ranges for IPv4 and IPv6 in custom MetaCallback feeds. As with other custom feeds, you must create feed data file in .csv format, and a feed definition file in .xml format.

**Note:** Using MetaCallback feeds with CIDR index ranges is supported only through the Advanced Configuration wizard or the REST interface.

The following example shows the content of both a .csv file and an .xml file for a MetaCallback feed using CIDR index ranges for IPv4 or IPv6.

### CSV File Content

```
192.168.0.0/24, Sydney
192.168.1.0/24, Melbourne
```

### XML File Content

```
<?xml version="1.0" encoding="UTF-8"?><FDF
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">
<FlatFileFeed name="ip_test" path="ip_test.csv" separator="," comment="#">
<MetaCallback name="DstIP" valuetype="IPv4" apptype="0" truncdomain="false">
<Meta name="ip.dst"/>
</MetaCallback>
<LanguageKeys>
<LanguageKey name="alert" valuetype="Text" />
</LanguageKeys>
<Fields>
<Field index="1" type="index" range="cidr"/>
<Field index="2" type="value" key="alert" />
</Fields>
</FlatFileFeed>
</FDF>
```




**Note:** To configure a CIDR index range for feeds with single or multiple MetaCallbacks of value type IPv4 or IPv6, the field of type index MUST contain a range attribute with range="cidr". Also, configuring "cidr" index ranges for feeds with MetaCallbacks of multiple different value types is not supported.

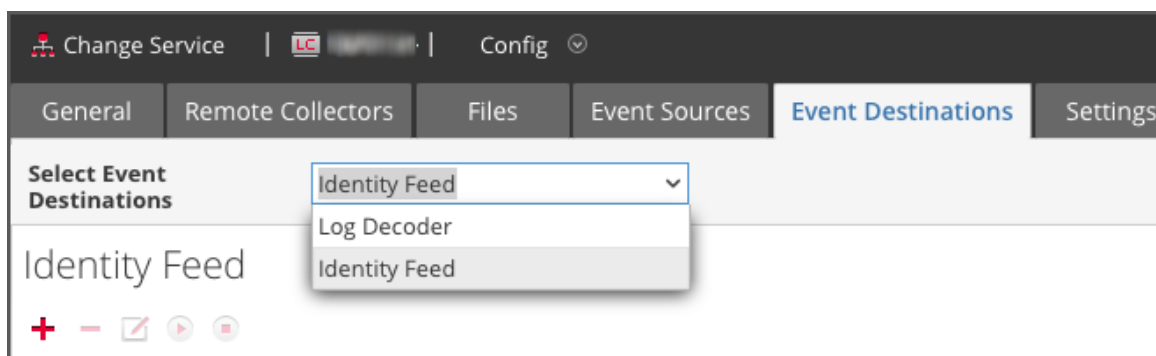



## Creating and Managing an Identity Feed

You can easily create an Identity feed and populate it to selected Decoders and Log Decoders. After completing this procedure, you will have created an Identity feed.

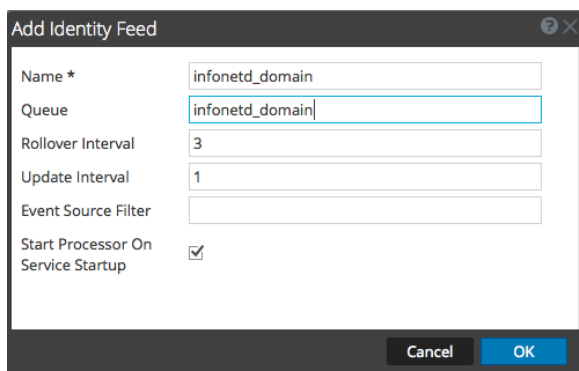
### To create an identity feed:

1. Add a destination for the feed.
  - a. Go to  (Admin) > Services and in the Services.
  - b. In the list of services, select a **Log Collector** service, and select   **View > Config**.
  - c. Select the **Event Destinations** tab.
  - d. In the Select **Event Destinations** field, select **Identity Feed**.



- e. Click  and enter a unique name for the feed.

The Queue name identifies the feed within the Log Collector. Use the name of the feed for the Queue.


 The screenshot shows a dialog box titled 'Add Identity Feed'. It contains several input fields: 'Name \*' with the value 'infonetd\_domain', 'Queue' with the value 'infonetd\_domain', 'Rollover Interval' with the value '3', and 'Update Interval' with the value '1'. There is also an empty 'Event Source Filter' field and a checked checkbox for 'Start Processor On Service Startup'. At the bottom, there are 'Cancel' and 'OK' buttons.

- f. Click **OK**.
2. Test generation of messages.
    - a. Have users log into Windows boxes on the domain to generate the appropriate log messages on the domain controllers for testing.

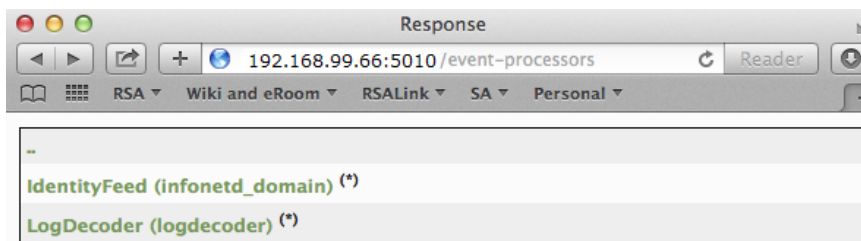
- b. Verify that data is written to the feed files. SSH to the Log Decoder/Collector or Virtual Log Collector being configured. Navigate to `/var/netwitness/logcollector/runtime/identity-feed` and verify that the `Identity_deploy` files are getting populated with data.

```
[root@tps-reports identity-feed]# pwd
/var/netwitness/logcollector/runtime/identity-feed
[root@tps-reports identity-feed]# ls -lah
total 20K
drwxr-xr-x. 2 root root 109 Nov  8 18:06 .
drwxr-xr-x. 8 root root 4.0K Nov 12 23:14 ..
-rw-r--r--. 1 root root 106 Nov 13 15:24 identity_deploy.csv
-rw-----. 1 root root 408 Nov 13 15:24 identity_deploy.feed
-rw-r--r--. 1 root root 981 Nov  8 09:06 identity_deploy.xml
-rw-r--r--. 1 root root 158 Nov 13 15:17 identitycache.csv
[root@tps-reports identity-feed]#
```

- c. Open up a web browser (Non-Internet Explorer browsers preferred) and log in to the REST interface of the Log Collector. Use administrative credentials when logging in. For example, if the IP address of your Log Collector is 192.168.99.66, the URL would be:

- SSL not enabled: **<http://192.168.99.66:50101/event-processors>**
- SSL enabled: **<https://192.168.99.66:50101/event-processors>**

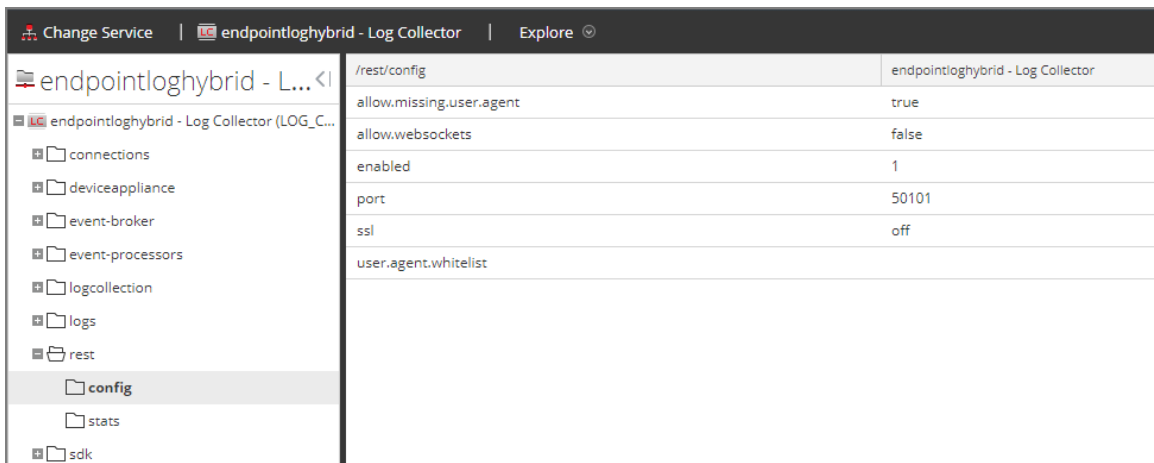
The browser screen should look like this:



The screen contains the name of the identity feed you created earlier (`infonetd_domain`, in this example).

For the identity feed to function correctly, port 50101 must be active on the Log Collector, and you must determine whether SSL encryption is active.

- d. Go to  (Admin) > Services > <Log Collector being setup>  > View > Explore.
- e. In the left pane, expand `rest` > `config`.



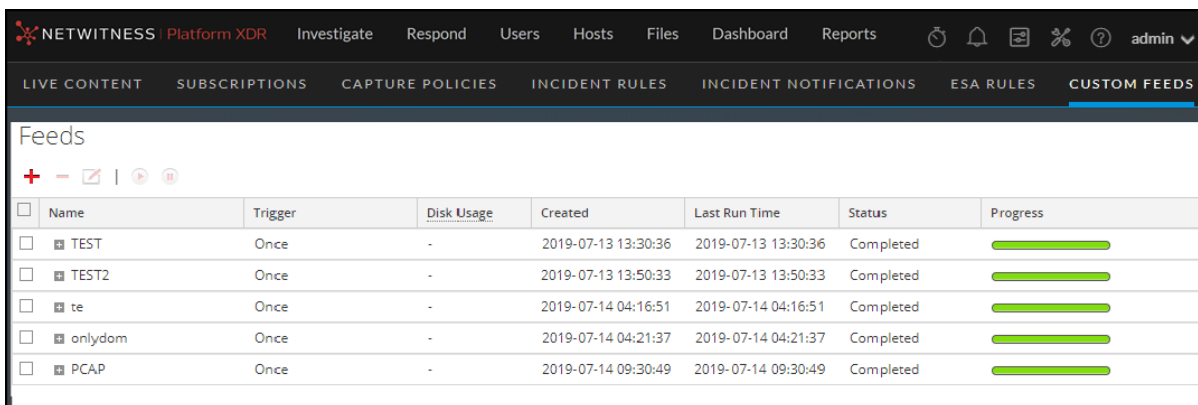
For REST to be active, **enabled** must be set to **1**.


- f. Note the value for **ssl**. If SSL should be enabled for your environment, this must be set to **on**.

**Note:** If you changed the setting for either the **enabled** or **ssl** option you must restart the Log Collector service before moving forward.

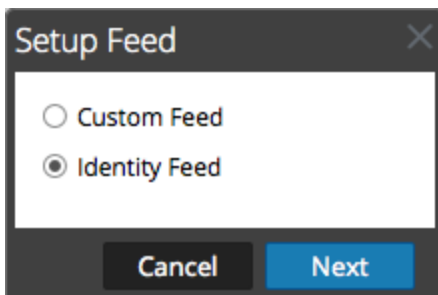
3. Go to  **(Configure) > Custom Feeds**.

The Feeds dialog is displayed.



4. In the toolbar, click .

The Setup Feed dialog is displayed.



5. Make sure **Identity Feed** is selected and click **Next**.

The Configure Identity Feed panel opens with the **Define Feed** tab displayed.

6. (Conditional) You can create an on-demand or recurring feed.
  - To define an on-demand Identity feed task that executes once, select **Adhoc** in the **Feed Task Type** field, type the feed **Name**, and browse for and open the feed.
  - To define a recurring Identity Feed task that executes on a recurring basis, select **Recurring** in the **Feed Task Type** field.

The **Define Feed** dialog includes the fields for a recurring feed.

**Note:** NetWitness verifies the location where the file is stored, so that NetWitness can check for the latest file automatically before each recurrence.

7. Enter a value and verify the URL field.
  - a. In the **URL** field, enter the URL where the feed data file is located. This is the REST API interface that was setup earlier. Make sure you have the following information to construct the URL:
    - The IP address of the Log Collector being used to construct the Identity Feed file.
    - The identity queue name, as set in [step 2c](#).
    - Whether or not SSL is enabled on the Log Collector REST port, as set in [step 2f](#).

You can construct this value as follows:

- SSL enabled: `https://<LogCollector>:50101/event-processors/<ID Event processor name>?msg=getFile&force-content-type=application/octet-stream&expiry=600`
- SSL not enabled: `http://<LogCollector>:50101/event-processors/<ID Event processor name>?msg=getFile&force-content-type=application/octet-stream&expiry=600`

So, using the example from earlier, the complete value that you would enter into this field is as follows:

```
http://192.168.99.66:50101/event-processors/infonetd_domain?msg=getFile&force-content-type=application/octet-stream&expiry=600?msg=getFile&force-content-type=application/octet-stream&expiry=600
```

- b. For the URL verification to work correctly, it is important that the NetWitness UI server can access the Log Collector's REST API port (50101). This can be tested by going to the NetWitness UI server via SSH. Once there, run the following command:

- SSL enabled: `curl -vk https://<ip of log collector>:50101`
- SSL not enabled: `curl -v http://<ip of log collector>:50101`

If the `curl` command does not connect then there may be a network firewall or routing issue between the NetWitness UI server and the Log Collector.

Example of a bad connection:

```
* About to connect() to 192.168.99.66 port 50105 (#0)
* Trying 192.168.99.66... No route to host
* couldn't connect to host
* Closing connection #0
curl: (7) couldn't connect to host
```

Example of a good connection:

```
* About to connect() to 192.168.99.66 port 50105 (#0)
* Trying 192.168.99.66... connected
* Connected to 192.168.99.66 (192.168.99.66) port 50105 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7
NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
> Host: 192.168.99.66:50105
> Accept: */*
>
< HTTP/1.1 401 Unauthorized
< Content-Length: 71
< Connection: Keep-Alive
< Pragma: no-cache
< Expires: -1
< Cache-Control: no-cache, no-store, must-revalidate
< WWW-Authenticate: Basic realm="NetWitness"
< Content-Type: text/xml; charset=utf-8
<
<?xml version="1.0" encoding="utf-8"?>
<error>401 Unauthorized</error>
* Connection #0 to host 192.168.99.66 left intact
* Closing connection #0
```

8. The REST API requires a username and password when attempting to pull the `identity_deploy.csv` file from the Log Collector. This can be any username and password that is available on the service itself. For more information, see the "Services Security View" topic in the *Hosts and Services Guide*.

To see which accounts are available, go to  (Admin) > Services > <log collector being setup> > Actions > View > Security.

Under the Users table, you see all the users that can be used in this step. It is suggested that a separate user account is created specifically for this setup, and is used nowhere else in the environment, for added security. For details, see "Add a User and Assign a Role" in the *System Security and User Management Guide*. (Go to the [NetWitness All Versions Documents](#) page and find NetWitness Platform guides to troubleshoot issues.)

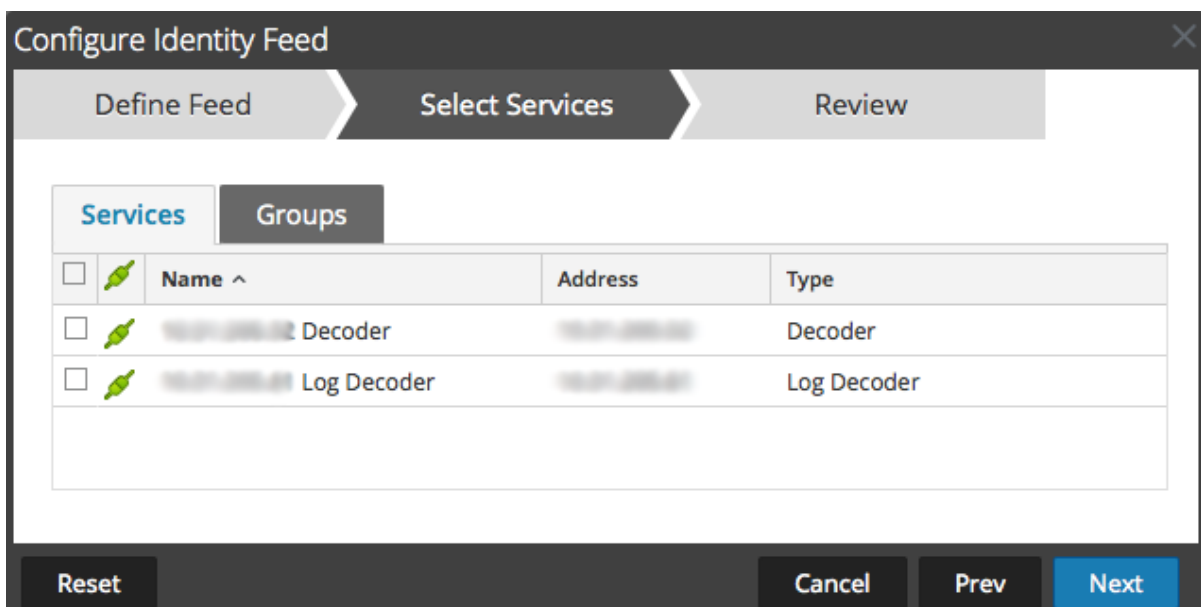
9. To define the recurrence interval, do one of the following:

- Specify the number of minutes, hours, or days between recurrences of the feed.
  - Enter the date range for the execution of the feed to recur, specify the **Start Date** and time and the **End Date** and time.
10. If using SSL encryption, you need to install the REST API SSL certificate for the Log Collector into the NetWitness UI server. For more information, see [Import the SSL Certificate](#).

If, after importing the SSL certificate, the verification of the URL still fails, see [Cannot Verify Identity Feed URL](#).

11. Click **Verify** to verify your identity feed configuration before you proceed to the Select Services dialog.
12. Click **Next**.

The Select Services dialog is displayed.



13. To identify services on which to deploy the feed, select one or more Decoders and Log Decoders and click **Next**.
14. Click the **Groups** tab, select a group, and click **Next**.

The Review dialog is displayed.

**Configure Identity Feed**

Define Feed    Select Services    Review

**Feed Details**

Name: Testing

Feed File: zip sample.zip

**Service Details**

Services: Decoder

Reset    Cancel    Prev    Next

**Note:** If a group of devices with Decoders and Log Decoders is used to create recurring or custom feeds and this group is deleted, you can edit the feed and add a new group to the feed.

15. Anytime before you click **Finish**, you can:
  - Click **Cancel** to close the wizard without saving your feed definition.
  - Click **Reset** to clear the data in the wizard.
  - Click **Next** to display the next form (if not viewing the last form).
  - Click **Prev** to display the previous form (if not viewing the first form).
16. Review the feed information, and if correct, click **Finish**.

Upon successful creation of the feed definition file, the Create Feed wizard closes, and the feed and corresponding token file are listed in the Feed grid and progress bar tracks completion. You can expand or collapse the entry to see how many services are included, and which services were successful.

Name	Trigger	Feed Size	Created	Last Run Time	Status	Progress
FILEHASH	Fetches STIX feeds from 2020-May-19 03:16, running every 5 minutes	0 bytes	2020-05-19 03:25:23	2020-05-22 05:16:01	Completed	<div style="width: 100%;"></div>
FILESTIX	Fetches STIX feeds from 2020-May-19 03:32, running every 5 minutes	0 bytes	2020-05-19 03:32:09	2020-05-22 05:12:09	Completed	<div style="width: 100%;"></div>
AllIndicatorsREST	Fetches STIX feeds from 2020-May-19 04:48, running every 5 minutes	0 bytes	2020-05-19 05:03:52	2020-05-22 05:13:26	Completed	<div style="width: 100%;"></div>
AllIndEdited	Fetches STIX feeds from 2020-May-19 05:13, running every 5 minutes	0 bytes	2020-05-19 05:13:54	2020-05-22 05:13:54	Completed	<div style="width: 100%;"></div>
TAXIServer1	Fetches STIX feeds from 2020-May-19 05:44, running every 5 minutes	288 bytes	2020-05-19 05:44:38	2020-05-22 05:14:38	Completed	<div style="width: 100%;"></div>

### Import the SSL Certificate

If SSL is configured on the Identity feed's Log Collector, follow these steps to import the Log Collector's SSL certificate into the NetWitness UI server key store. If this certificate is not imported, the NetWitness UI server will be unable to pull the Identify feed file from the Log Collector.

1. To pull the SSL certificate off the Log Collector, SSH into the NetWitness UI server and run the following command:

```
echo -n | openssl s_client -connect <HOST>:<PORT> | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > /tmp/<SERVERNAME>.cert
```

This command saves the SSL certificate to /tmp/<SERVERNAME>.cert. For example:

```
echo -n | openssl s_client -connect 192.168.99.66:50101 | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > /tmp/logcollector.cert
```

2. To import the SSL certificate into the NetWitness UI server, SSH into the UI server and run the following command:

```
keytool -importcert -alias <name an alias for the cert> -file <the cert file pathname> -keystore /etc/pki/java/cacerts
```

For example:

```
keytool -importcert -alias logcollector01 -file /tmp/logcollector.cert -keystore /etc/pki/java/cacerts
```

3. The system requests a password. Enter the password for the keystore on the NetWitness UI server, not for the jetty keystore. The default password is **changeit**.
4. Restart **jetty** to allow jetty to read the new certificate in the store.

### Cannot Verify Identity Feed URL

If the Identity feed URL cannot be verified, and you are using SSL, make sure you followed the steps in [Import the SSL Certificate](#).

If there are issues, it is possible that the internal name of the certificate does not match the hostname of the Log Collector. The following procedure checks this.

1. SSH to the NetWitness UI server.
2. Run the following command to output the CN name of the SSL cert:

```
echo -n | openssl s_client -connect <log decoder>:50101 | sed -ne '/BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
```

For example:

```
echo -n | openssl s_client -connect salogdecoder01:50101 | sed -ne '/BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
```

3. Retrieve the CN name of the SSL certificate.

```
depth=0 C = US, CN = NetWitness-SALogdecoder01 ←
verify error:num=18:self signed certificate
verify return:1
depth=0 C = US, CN = NetWitness-SALogdecoder01
verify return:1
-----BEGIN CERTIFICATE-----
MIIC2zCCAcOgAwIBAgIBADANBgkqhkiG9w0BAQQFADAxMQswCQYDVQQGEwJVUzEi
MCAGAlUEAxMZTmV0V210bmVzcy1TQWxvZ2R1Y29kZXIwMTAeFw0xNDAxMTEwMDM1
```



4. Edit the `/etc/hosts` file and add the IP address and CN name to the file.

```
# Created by NetWitness Installer on Fri Jan 10 21:42:10 UTC 2014
127.0.0.1 SAserver01 localhost.localdom localhost
::1 SAserver01 localhost.localdom localhost ip6-localhost ip6-loopback
192.168.10.23 NetWitness-SALogdecoder01
```

5. Restart the network service on the appliance.
6. Confirm that the name placed in the `/etc/hosts` file is used instead of the FQDN or IP address in the Identity feed URL.
7. Re-verify the Identity feed URL.

#### Investigating an Identity Feed

An identity feed tracks interactive log on events from the Windows operating system. Identity feeds do not track interactive log off events.

In order for an identity feed to process events and tag them, the events need to be collected using a Windows Log Collection module where an Active Domain Controller or non-Domain Controller is configured. Note that identity feeds can only be processed via an Identity Feed Event Processor.

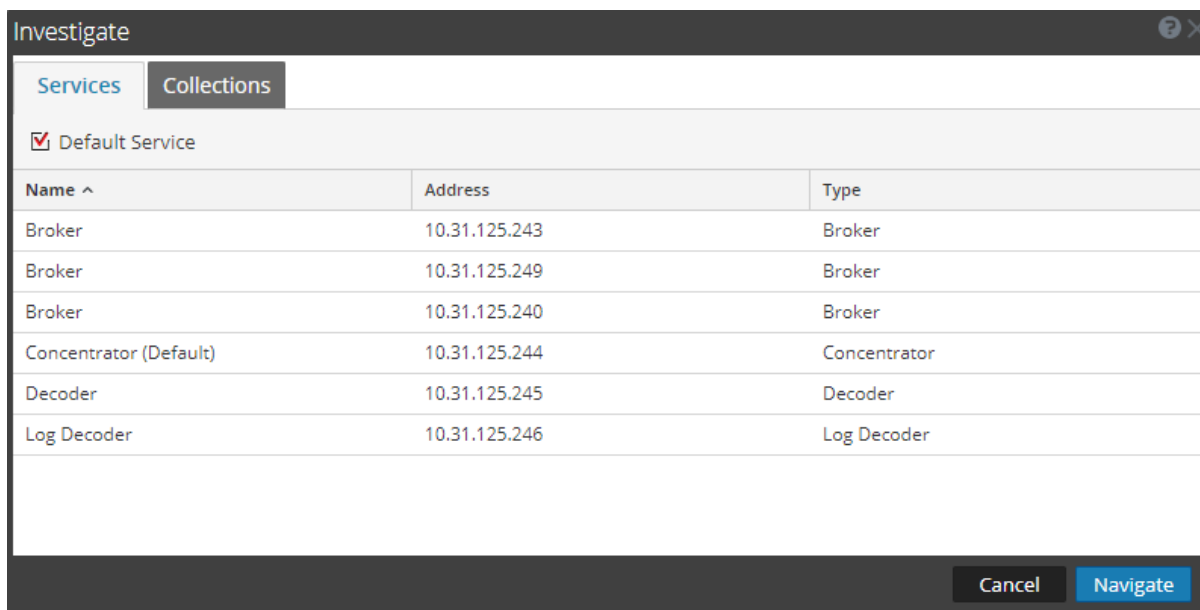
**Note:** An identity feed only tracks one log in at a time. If two users log in to a system at the same time, the second user will overwrite the first user's data in the identity feed.

Once you have created an identity feed, you can view the results by investigating the feed.

#### To investigate a configured identity feed:

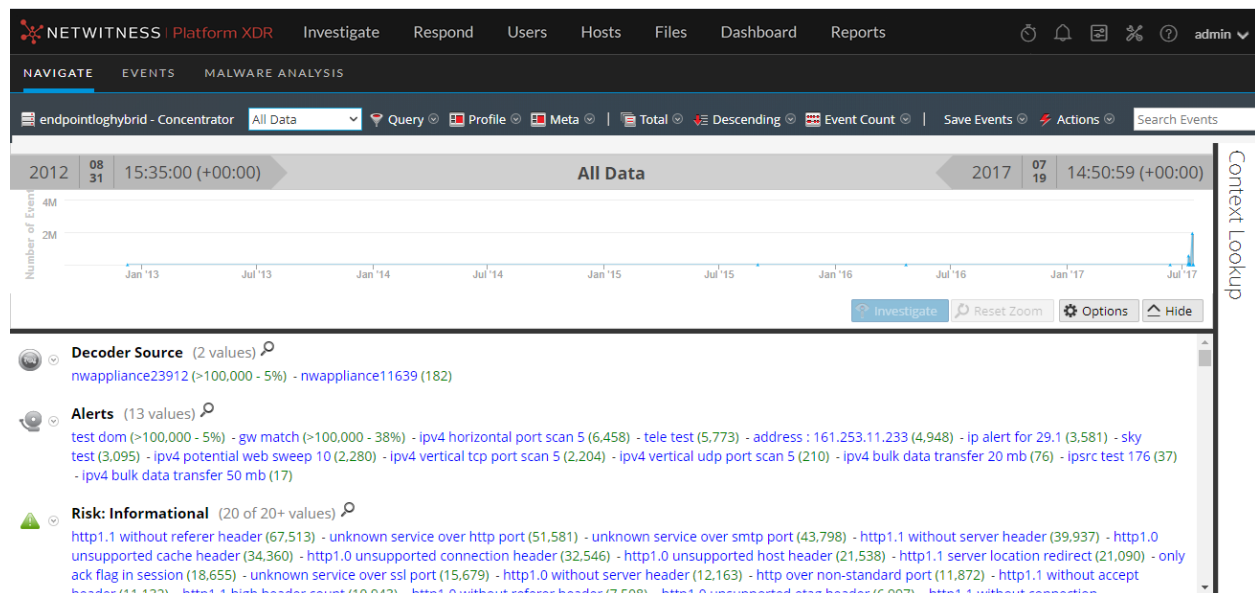
1. Go to **Investigate** > **Navigate**.

If no default service is selected, the Investigate dialog is displayed.



2. Select a service, usually a Concentrator, and click **Navigate**.
3. Select **Load Values** to retrieve meta data.

In the Values panel, scroll down to find the Meta Keys:



The identity feed provides information to selected Decoders and Log Decoders. It associates the Host IP data from the Windows operating system to the user logging into that Host in order to tag all logs associated with that IP and investigate.

## Editing a Feed

This topic provides instructions for editing a custom feed using the Custom Feed Wizard.

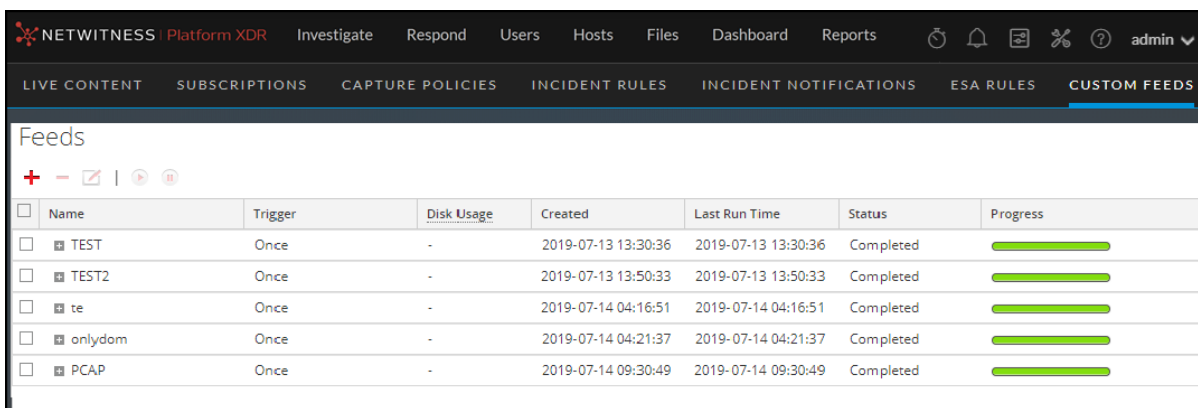
After you edit a feed:

- The feed (.zip format) or the file used to create the feed (.csv or .xml) has been downloaded and edited.
- The feed has been recreated with the updated file and new feed specifications.


### To edit an existing feed:

1. Go to  (Configure) > CUSTOM FEEDS.

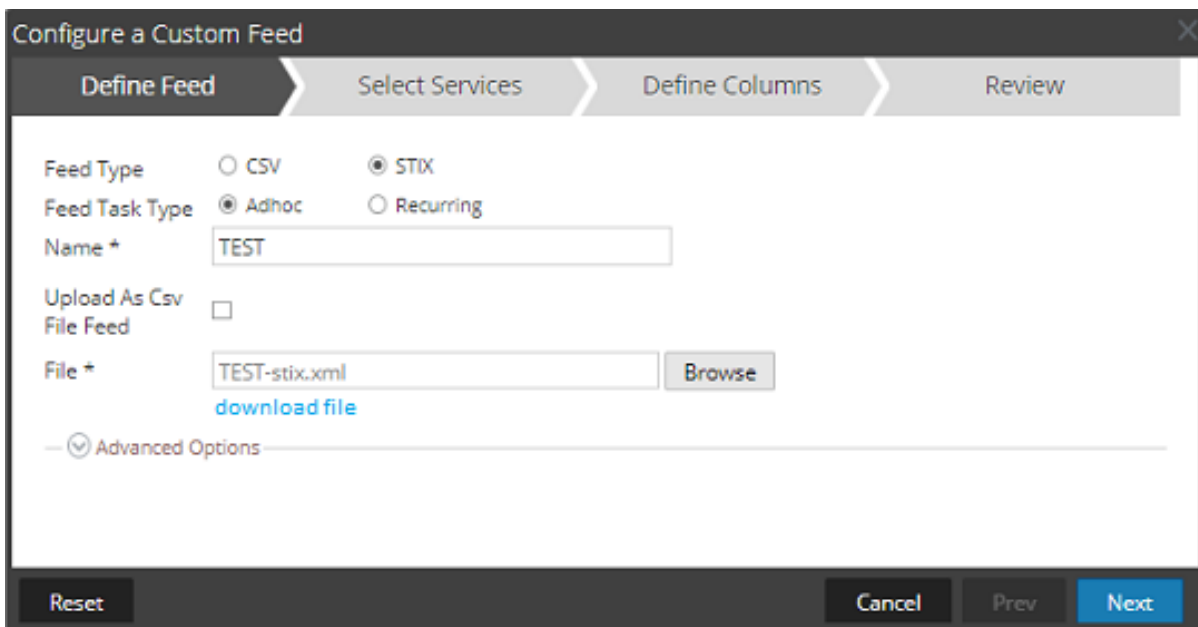
The Custom Feeds dialog is displayed.



Name	Trigger	Disk Usage	Created	Last Run Time	Status	Progress
TEST	Once	-	2019-07-13 13:30:36	2019-07-13 13:30:36	Completed	<div style="width: 100%;"></div>
TEST2	Once	-	2019-07-13 13:50:33	2019-07-13 13:50:33	Completed	<div style="width: 100%;"></div>
te	Once	-	2019-07-14 04:16:51	2019-07-14 04:16:51	Completed	<div style="width: 100%;"></div>
onlydom	Once	-	2019-07-14 04:21:37	2019-07-14 04:21:37	Completed	<div style="width: 100%;"></div>
PCAP	Once	-	2019-07-14 09:30:49	2019-07-14 09:30:49	Completed	<div style="width: 100%;"></div>

2. In the toolbar, select a feed and click .

The Configure Custom Feed or Configure Identity Feed panel opens in the Custom Feed wizard.



Configure a Custom Feed

Define Feed | Select Services | Define Columns | Review

Feed Type:  CSV  STIX

Feed Task Type:  Adhoc  Recurring

Name:

Upload As Csv File Feed:

File:   [download file](#)

Advanced Options:

Reset Cancel Prev Next

3. If you want to edit the feed file:
  - a. Click **download file**.

For an Identity feed, the .zip file is downloaded. For a custom feed, the .csv or .xml file is downloaded to your local file system.
  - b. Edit and save the file.
  - c. In the **Define Feed** tab, browse for and open the edited file.
4. Edit any other parameters in the **Define Feed** tab, **Select Services** tab, and **Define Columns** tab that apply to the type of feed.
5. Anytime before you click **Finish**, you can:
  - Click **Cancel** to close the wizard without saving your changes.
  - Click **Reset** to clear the data in the wizard.
  - Click **Next** to display the next form (if not viewing the last form).
  - Click **Prev** to display the previous dialog (if not viewing the first form).
6. In the **Review** tab, review the feed information, and if correct, click **Finish**.

The feed is added to the feeds list and progress bar tracks completion. Upon successful creation of the feed definition file, the Create Feed wizard closes, and the feed and corresponding token file is listed in the Feeds list. You can expand or collapse the entry to see how many services are included, and which services are successful.

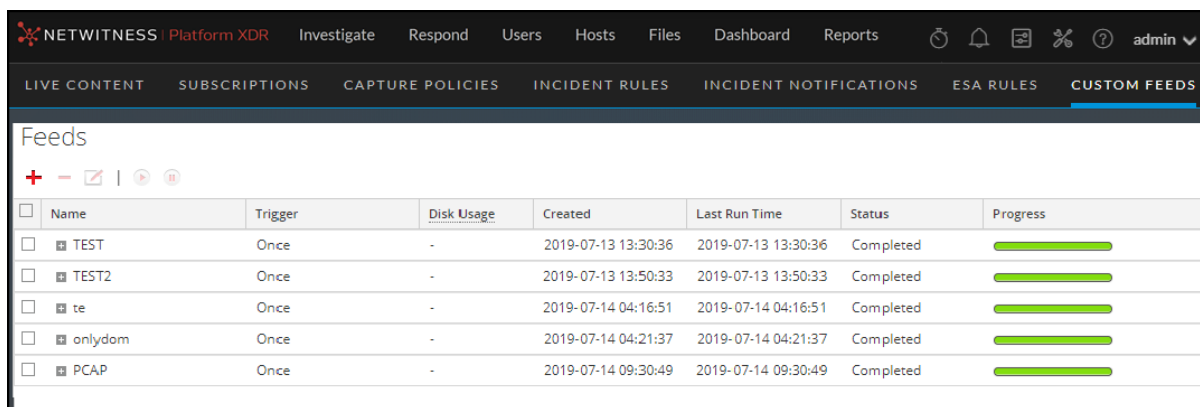
## Removing a Feed

This topic provides instructions for removing a feed. You might want to remove a feed when some or all of the information in the feed is no longer useful for your organization.

### To remove a feed:

1. Go to  (Configure) > CUSTOM FEEDS.

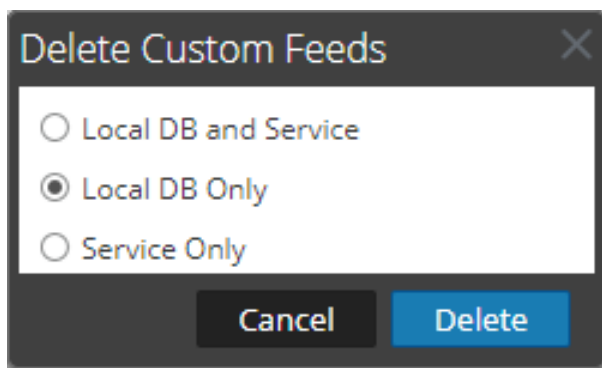
The Custom Feeds dialog is displayed.



<input type="checkbox"/>	Name	Trigger	Disk Usage	Created	Last Run Time	Status	Progress
<input type="checkbox"/>	TEST	Once	-	2019-07-13 13:30:36	2019-07-13 13:30:36	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>
<input type="checkbox"/>	TEST2	Once	-	2019-07-13 13:50:33	2019-07-13 13:50:33	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>
<input type="checkbox"/>	te	Once	-	2019-07-14 04:16:51	2019-07-14 04:16:51	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>
<input type="checkbox"/>	onlydom	Once	-	2019-07-14 04:21:37	2019-07-14 04:21:37	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>
<input type="checkbox"/>	PCAP	Once	-	2019-07-14 09:30:49	2019-07-14 09:30:49	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>

2. In the toolbar, select a feed and click .

The Delete Custom Feeds dialog is displayed.



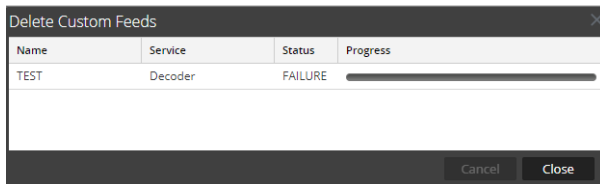
You can select one of the following options to delete the feed:

- If you choose to delete the feed from **Local DB and Service**, the feed is deleted from both the service and the local NetWitness box. The deleted feed will no longer be seen on the NetWitness user interface.
- If you choose to delete the feed from **Local DB Only**, the feed is deleted from the local NetWitness box. The deleted feed will not be seen on the NetWitness user interface; however, the last deployed version of the feeds will be present on the service. The undeployed feeds will be deleted forever.
- If you choose to delete the feed from **Service Only**, the feed is deleted from the service. The deleted feed will appear on the NetWitness user interface and can be deployed again.

3. Select which feed you want to delete and click **Delete**.

A warning dialog is displayed.

4. Click **yes** to confirm that you want to delete the feed from the selected areas.



## Subscribing to Live Resources

This section describes subscriptions in Live.

Threats and the corporate landscape change over time. NetWitness periodically reviews existing content to determine whether it needs to be updated based upon current campaigns, or has become irrelevant due to changes in technology or attack techniques and tools.

You can discover new content by using the What's New dashlet within the Default Dashboard, or by searching through NetWitness Live by data range since last deployed. Be sure to subscribe to any content for which you want to receive update notifications.


### Subscription Updates

When you view resources in the Matching Resources panel of the Live Content view, there is a column named **Updated**:

Matching Resources						
Show Results  Details  Deploy  Subscribe  Package						
<input type="checkbox"/>	Subscribed	Name	Created	Updated	Type	Description
<input type="checkbox"/>	no	Advanced Windows Execut...	2012-02-09 4:50 PM	2014-03-20 3:58 PM	FlexParser	Legacy: Intend
<input type="checkbox"/>	no	Fingerprint Windows MSI	2012-02-09 4:51 PM	2012-02-09 4:51 PM	FlexParser	Legacy: Intend
<input type="checkbox"/>	no	Microsoft Windows	2018-03-27 1:46 PM	2018-03-27 1:47 PM	Log Device	Log device cor
<input type="checkbox"/>	yes	windows_executable	2013-10-18 1:53 PM	2017-11-13 2:35 PM	Lua Parser	Identifies winc
<input type="checkbox"/>	no	Windows Command Shell	2012-02-09 4:51 PM	2013-08-27 7:08 AM	FlexParser	Legacy: Intend
<input type="checkbox"/>	yes	Lateral Movement Indicato...	2016-03-09 12:54 AM	2018-07-31 7:59 PM	NetWitness Report	Report display
<input type="checkbox"/>	yes	windows_command_shell_L...	2013-10-18 1:55 PM	2016-11-14 6:40 PM	Lua Parser	Identifies Micr
<input type="checkbox"/>	yes	Windows Credential Harves...	2016-03-09 12:54 AM	2016-03-09 12:54 AM	NetWitness Rule	This rule moni
<input type="checkbox"/>	no	Windows Process Parent C...	2018-05-11 7:34 PM	2018-05-11 7:34 PM	NetWitness Rule	There are sets
<input type="checkbox"/>	yes	Windows NTLM Network Lo...	2016-03-09 12:54 AM	2016-03-09 12:54 AM	NetWitness Rule	Indicates a po
<input type="checkbox"/>	no	Autoruns and Scheduled Ta...	2018-05-11 7:33 PM	2018-05-11 7:33 PM	NetWitness Rule	Attackers will
<input type="checkbox"/>	no	Windows Events (ER)	2014-02-14 3:54 AM	2018-03-27 8:30 AM	Log Device	Log device cor
<input type="checkbox"/>	no	Windows Events (NIC)	2014-02-14 3:55 AM	2018-09-03 12:11 PM	Log Device	Log device cor


66 Matching Resources

This value is also displayed when you select the detailed view for a resource. Every time a resource changes, its **Updated** value changes to match the specific update. If you are subscribed to a resource, and it gets updated, your system is automatically updated with the latest version, and you receive a




notification. You can view your notifications by clicking the Notification icon, , from anywhere in the NetWitness UI.

The screenshot displays the NetWitness Platform XDR interface. The top navigation bar includes 'Investigate', 'Respond', 'Users', 'Hosts', 'Files', 'Dashboard', and 'Reports'. Below this, the 'LIVE CONTENT' section is active, showing 'SUBSCRIPTIONS', 'CAPTURE POLICIES', 'INCIDENT RULES', and 'INCIDENT NOTIFICATIONS'. The main area is divided into 'Search Criteria' on the left and 'Matching Resources' on the right. The 'Search Criteria' panel includes 'Keywords', 'Category' (with options like FEATURED, THREAT, IDENTITY, Authentication, Accounting, ASSURANCE, OPERATIONS, SPECTRUM, MALWARE ANALYSIS), and 'Resource Types'. The 'Matching Resources' table has columns for 'Subscribed', 'Name', 'Created', and 'Updated'. A 'Notifications' panel is open on the right, showing alerts for 'Service Added' and 'Entitlement Expiration'.

Subscribed	Name	Created	Updated
<input type="checkbox"/>	LDAP	2013-09-12 2:21 PM	2017-11-21 7:15 PM
<input type="checkbox"/>	Kerberos	2013-09-12 2:21 PM	2018-05-24 7:26 PM
<input type="checkbox"/>	NWFL_account:login-succe...	2012-04-20 5:01 PM	2015-12-30 8:52 AM
<input type="checkbox"/>	Multiple Login Failures Due...	2013-12-24 11:25 AM	2016-12-14 8:17 PM
<input type="checkbox"/>	Multiple Failed Logins to SI...	2014-02-27 11:23 AM	2016-12-14 8:17 PM
<input type="checkbox"/>	VM Clone After Multiple Ro...	2014-01-22 6:16 PM	2016-12-14 8:17 PM
<input type="checkbox"/>	Multiple Service Connectio...	2014-02-27 11:23 AM	2016-12-14 8:18 PM
<input type="checkbox"/>	Remote Data Harvesting	2014-08-16 9:01 AM	2016-12-14 8:19 PM
<input type="checkbox"/>	NWFL_account:login-failure	2012-04-20 4:56 PM	2014-08-16 9:20 AM
<input type="checkbox"/>	NWFL_account:login-and-lo...	2012-04-20 5:03 PM	2014-08-16 9:20 AM
<input type="checkbox"/>	NWFL_account:login-success	2012-04-20 5:00 PM	2014-08-16 9:20 AM
<input type="checkbox"/>	NWFL_account:logout	2012-04-20 5:11 PM	2014-08-16 9:20 AM
<input type="checkbox"/>	Malicious Account Creation...	2014-02-27 11:23 AM	2016-12-14 8:18 PM
<input type="checkbox"/>	NTLMSSP_Iua	2013-09-16 3:06 AM	2015-05-30 5:06 AM

You can also get email notifications when subscribed resources are updated. System Administrators can add email addresses in the  (Admin) > SYSTEM > Live Services view. For more information, see the "Live Services Configuration Panel" topic in the *System Configuration Guide*.

### Adding Subscribed Resources for Deployment to Services



1. Go to  (Configure) > Subscriptions > Deployments.
2. In the **Groups** panel, select a group.  
Subscribed resources, if any, are listed in the Deployments tab Subscriptions panel.
3. In the **Subscriptions** panel, click  .  
The Add Subscription dialog, which lists subscriptions available for deployment, is displayed.
4. Select the subscribed resources that you want to deploy to the services group.
5. Click **Save**.  
The dialog closes and the subscriptions are added to the listing in the Deployments tab, Subscriptions panel. This stages the resources for deployment at the next synchronization.
6. You can click the Synchronize icon,  , to immediately synchronize your changes.

### Deleting a Subscription

When you delete a subscription to a resource, deployed instances of the resource are not deleted. The deployed resource remains on services until explicitly removed, but the resource is no longer synchronized with the resource in NetWitness Live.



**To delete a subscription:**



1. Go to  (Configure) > Subscriptions.
2. In the **Subscriptions** tab, select the subscriptions you want to delete.
3. Click , then choose **Delete** to delete your selected resources or **Delete All** delete all subscriptions. A dialog asks for confirmation that you want to delete the subscription.
4. To confirm removal, click **Yes**.  
Your selected subscriptions are deleted from the subscriptions list, but any deployed instances of the subscribed resource remain on the services.

**Removing Subscribed Resources from the Deployments Subscriptions Grid**

Subscriptions that are selected for deployment to a service group are deployed during synchronization.

You can remove subscriptions from the Live  (Configure) > Subscriptions > Deployments panel, but any that have actually been deployed to services remain deployed until someone removes them.



**To remove resources from the Deployments tab Subscriptions panel:**

1. Go to  (Configure) > Subscriptions > Deployments
2. In the **Groups** panel, select a group.  
Subscribed resources, if any, are listed in the Subscriptions panel.
3. In the Subscriptions panel, click .  
A dialog requests confirmation that you want to delete the resource from the service group. The resource is removed from the Deployments tab Subscriptions panel, but is not removed from services on which it is deployed.

**Subscribe and Unsubscribe to a Resource**





When you subscribe to resources, you will receive notification when new versions of the resources are available.

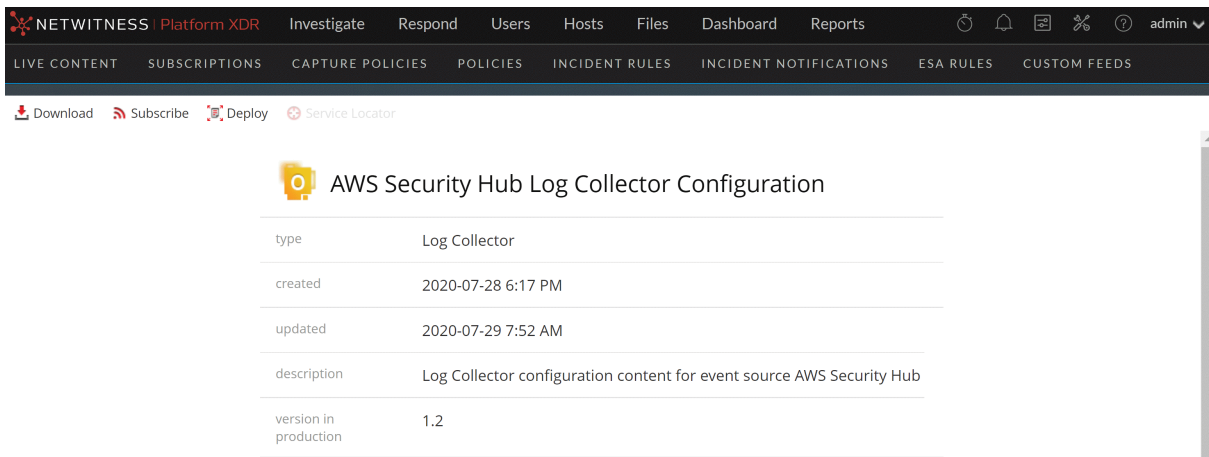
**To subscribe to a resource:**


1. Go to  (Configure) > Live Content.
2. In the **Search Criteria** panel, specify search criteria and click **Search**.
3. Select one or more resources and click  **Subscribe**.  
A confirmation dialog is displayed: **By subscribing to these resources, you are indicating that you wish to receive notification when new versions are available.**
4. To confirm that you want to subscribe to the resource, click **OK**.  
The resource is added to the subscriptions managed in the Subscriptions tab and is available for deployment in the Deployments tab.

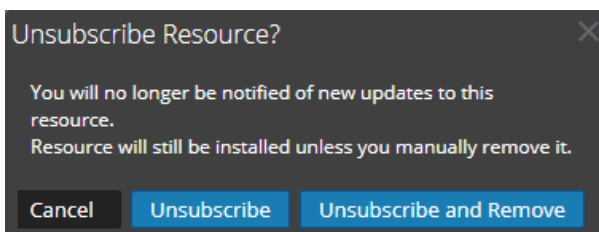
When unsubscribing from a resource, you have the option to leave the resource on services on which it is deployed or to remove it from services.

### To unsubscribe from a resource:

1. Open a detailed view of a resource in one of the following ways:
  - Perform a search,  **(Configure)** > **Live Content** > enter search criteria, then select the resource in the Matching Resources panel, then click  **Details**.
  - View subscriptions,  **(Configure)** > **Subscriptions**, select the resource from the Subscriptions list, then click  **Details**.



2. With the detailed view of a resource displayed, click  **Unsubscribe**.  
A confirmation dialog is displayed.



3. Do one of the following:
  - To confirm that you want to unsubscribe from the resource and leave it on the services where it is deployed, click **Unsubscribe**.
  - To confirm that you want to unsubscribe from the resource and remove it from the services where it is deployed, click **Unsubscribe and Remove from Services**.
  - To close the dialog without unsubscribing, click **Cancel**.

The selected action is applied.

### Viewing Subscribed Resources Selected to Deploy on Services

In the  **(Configure)** > **Subscriptions** > **Deployments** tab you can view subscribed resources that have been selected for deployment on services.

#### **To view subscribed resources that have been selected for deployment on services:**

In the **Groups** panel, select a group, and expand it to view services in the group. The resource subscriptions selected for deployment are listed in the Deployments tab Subscriptions panel.

## Miscellaneous Live Services Procedures

This section describes several other procedures.

### Displaying Resource Details in Live Resource View

After you select a resource (in the Live Resource View), you can view its detailed information.

To open a separate tab in the Live Resource view with details of a selected resource, do one of the following:

- If you are viewing the results in **Show Results > Detailed view**, click the resource type icon or the resource name.

The screenshot displays the NetWitness Platform XDR interface. The top navigation bar includes 'NETWITNESS Platform XDR' and menu items: 'Investigate', 'Respond', 'Users', 'Hosts', 'Files', 'Dashboard', and 'Reports'. A secondary navigation bar shows 'LIVE CONTENT' as the active section, with other options like 'SUBSCRIPTIONS', 'CAPTURE POLICIES', 'POLICIES', 'INCIDENT RULES', 'INCIDENT NOTIFICATIONS', 'ESA RULES', 'CUSTOM FEEDS', and 'LOG PARSER RULES'. The main interface is split into two panels. The left panel, 'Search Criteria', contains a 'Keywords' input field, a 'Category' section with checkboxes for 'FEATURED', 'THREAT', 'IDENTITY', 'ASSURANCE', 'OPERATIONS', 'SPECTRUM', and 'MALWARE ANALYSIS', a 'Resource Types' section with dropdowns for 'Malware Rules' and 'Log Collector', a 'Medium' dropdown, and a 'Required Meta Keys' input field. A 'Search' button is located at the bottom of this panel. The right panel, 'Matching Resources', shows a list of resources. At the top of this panel are controls for 'Show Results', 'Details', 'Deploy', 'Subscribe', and 'Package'. The list includes: 'RSA Malware PE Artifacts' (type Malware Rules, updated 2018-05-04 11:11 PM, version 0.2, size 74.5 KB, subscribed no, description: Yara IOCs which statically analyze Windows PE file artifacts for signs of malware), 'RSA Malware PE Packers' (type Malware Rules, updated 2013-11-21 9:07 PM, version 0.1, size 93.97 KB, subscribed no, description: Yara IOCs which statically analyze Windows PE files to identify Common Packers), 'RSA Malware PDF Artifacts' (type Malware Rules, updated 2013-11-21 9:07 PM, version 0.1, size 587 B, subscribed no, description: Yara IOCs which statically analyze PDF file artifacts for signs of malware), 'McKesson HPF Log Collector Configuration' (type Log Collector, updated 2017-09-13 5:09 PM, version 0.2, size 1.42 KB, subscribed no, description: Log Collector configuration content for event source McKesson HPF, tags: event analysis, operations, log analysis), and 'SAP ERP Central Component Log Collector Configuration' (type Log Collector, updated 2017-09-13 5:10 PM, version 0.2, size 1.24 KB, subscribed no, description: Log Collector configuration content for event source SAP ERP Central Component, tags: event analysis, operations, log analysis). At the bottom of the list, it indicates '191 Matching Resources'.

- If you are viewing the results in **Show Results > Grid view**, double-click a resource or select a




resource and click **Details**.

The screenshot displays the NetWitness Platform XDR interface. The top navigation bar includes 'Investigate', 'Respond', 'Users', 'Hosts', 'Files', 'Dashboard', and 'Reports'. Below this, a secondary navigation bar lists various content types: 'LIVE CONTENT', 'SUBSCRIPTIONS', 'CAPTURE POLICIES', 'POLICIES', 'INCIDENT RULES', 'INCIDENT NOTIFICATIONS', 'ESA RULES', and 'CUSTOM FEEDS'. The main interface is split into two panels: 'Search Criteria' on the left and 'Matching Resources' on the right. The 'Search Criteria' panel includes fields for 'Keywords', 'Category' (with a tree view showing 'FEATURED', 'THREAT', 'IDENTITY', 'ASSURANCE', 'OPERATIONS', 'SPECTRUM', and 'MALWARE ANALYSIS'), 'Resource Types', 'Medium', 'Required Meta Keys', 'Generated Meta Values', and date pickers for 'Resource Created Date' and 'Resource Modified Date'. The 'Matching Resources' panel shows a table of results with columns for 'Subscribed', 'Name', 'Created', 'Updated', 'Type', and 'Description'. The table lists various resources such as 'RSA OSINT IP Threat Intel F...', 'Powershell Runs Command...', 'Runs ACL Management Tool', and 'AWS Security Hub Log Colle...'. At the bottom of the table, it indicates '663 Matching Resources'.

## Downloading a Resource

You can download a single resource from the [Live Resource View](#).

### To download a resource:

1. Go to  (Configure) > Live Content.
2. In the **Search Criteria** panel, enter the criteria needed to return the resource you want to download.
3. Select a single resource, then click  **Details**.
4. Click  **Download**.

The resource is saved as a ZIP archive to your local Downloads folder.

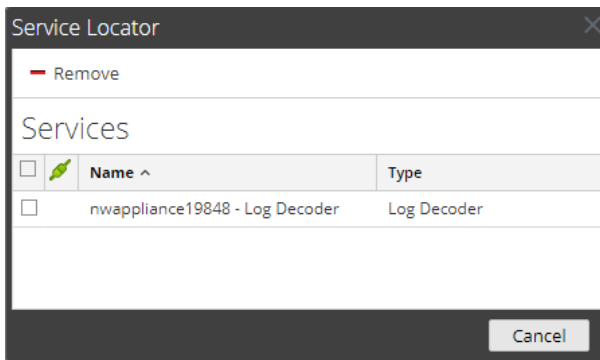
## Locating and Removing a Deployed Resource from Services

You can locate and remove a deployed resource from services from the [Live Resource View](#).

### To view a list of services on which a resource is deployed:

1. With a resource displayed in the **Resource View**, click  **Service Locator**.

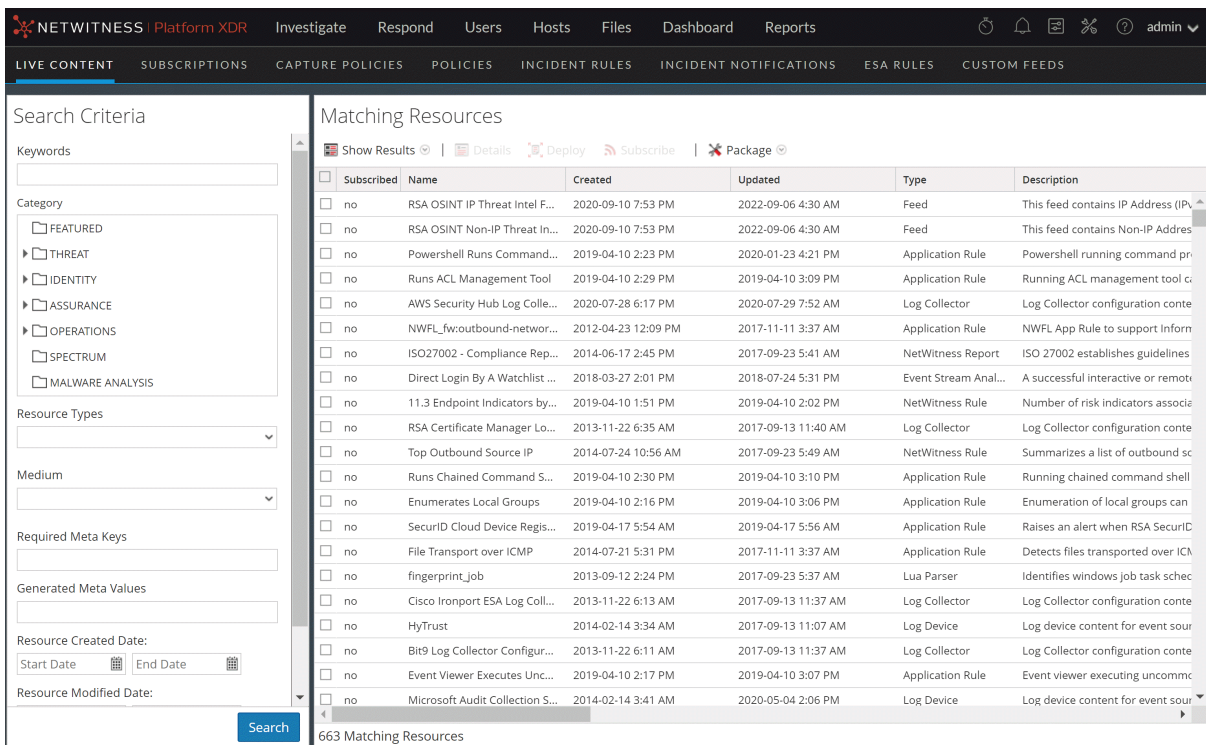
The Service Locator dialog is displayed.



2. Select one or more services in the **Services** list.
  3. Click **-**.
- The resource is removed from the selected services.

### Showing Results as a List or in Detail

1. Select **Show Results > Grid** to change to grid results when viewing detailed results.




2. Select **Show Results > Detailed** to change to detailed results when viewing grid results.

The screenshot displays the NETWITNESS Platform XDR interface. The top navigation bar includes 'Investigate', 'Respond', 'Users', 'Hosts', 'Files', 'Dashboard', and 'Reports'. Below this, a secondary navigation bar lists various content types: 'LIVE CONTENT', 'SUBSCRIPTIONS', 'CAPTURE POLICIES', 'POLICIES', 'INCIDENT RULES', 'INCIDENT NOTIFICATIONS', 'ESA RULES', 'CUSTOM FEEDS', and 'LOG PARSER RULES'. The main interface is split into two panels. The left panel, titled 'Search Criteria', contains a 'Keywords' search box, a 'Category' list with options like 'FEATURED', 'THREAT', 'IDENTITY', 'ASSURANCE', 'OPERATIONS', 'SPECTRUM', and 'MALWARE ANALYSIS', and a 'Resource Types' dropdown menu currently set to 'Malware Rules'. The right panel, titled 'Matching Resources', shows a list of results with columns for 'Show Results', 'Details', 'Deploy', 'Subscribe', and 'Package'. The first three results are 'RSA Malware PE Artifacts', 'RSA Malware PE Packers', and 'RSA Malware PDF Artifacts', all of type 'Malware Rules'. The next two are 'McKesson HPF Log Collector Configuration' and 'SAP ERP Central Component Log Collector Configuration', both of type 'Log Collector'. At the bottom of the right panel, it indicates '191 Matching Resources'.

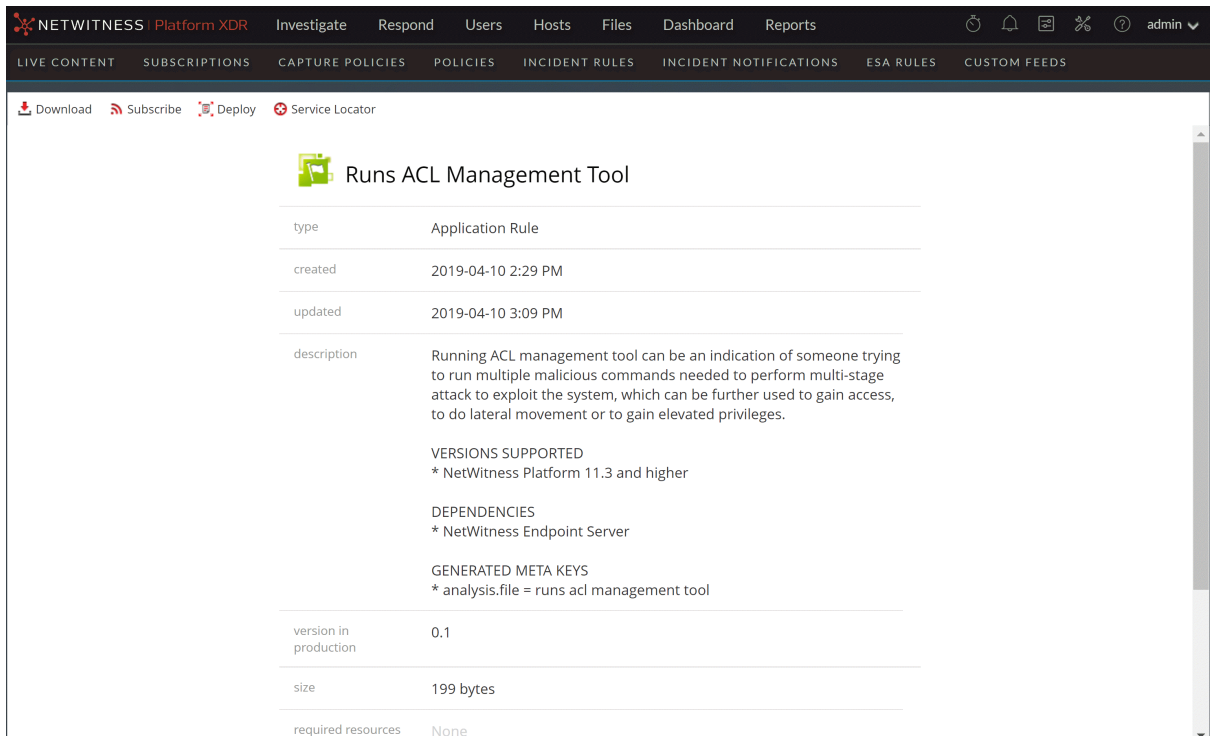
## Viewing Resource Details

You can display detailed information about a subscribed resource in the Resource View.

### To view details:

1. In the **Subscriptions** tab, select a single subscription.
2. Click  **Details**.

The details of the resource are displayed in the Resource View.



The screenshot displays the NetWitness Platform XDR interface. The top navigation bar includes 'NETWITNESS Platform XDR' and various menu items: Investigate, Respond, Users, Hosts, Files, Dashboard, Reports. A secondary navigation bar lists: LIVE CONTENT, SUBSCRIPTIONS, CAPTURE POLICIES, POLICIES, INCIDENT RULES, INCIDENT NOTIFICATIONS, ESA RULES, CUSTOM FEEDS. Below the navigation, there are action buttons: Download, Subscribe, Deploy, and Service Locator. The main content area shows the details for a resource titled 'Runs ACL Management Tool'.

Field	Value
type	Application Rule
created	2019-04-10 2:29 PM
updated	2019-04-10 3:09 PM
description	<p>Running ACL management tool can be an indication of someone trying to run multiple malicious commands needed to perform multi-stage attack to exploit the system, which can be further used to gain access, to do lateral movement or to gain elevated privileges.</p> <p><b>VERSIONS SUPPORTED</b> * NetWitness Platform 11.3 and higher</p> <p><b>DEPENDENCIES</b> * NetWitness Endpoint Server</p> <p><b>GENERATED META KEYS</b> * analysis.file = runs acl management tool</p>
version in production	0.1
size	199 bytes
required resources	None



## References

This topic is a collection of references, which describe the user interface and more detailed information about how Live works in NetWitness. These topics are presented in alphabetical order.

## Live Configure View


In the Live Configure view, NetWitness provides integrated tools for managing Live resources. You can manage resource subscriptions, deployments to services and discontinued resources. The required role to access this view is **Configure Live Resources**. For a high-level description of how to use the different views in NetWitness Live, please read [Live Services Management](#).

To access this view, navigate to  **(Configure) > Subscriptions**. The view has three tabs: [Deployments Tab](#), [Subscriptions Tab](#), and [Discontinued Resources Tab](#).

## Deployments Tab

The Deployments tab provides a user interface in the Live Configure view for:


- Viewing subscribed resources that are selected for deployment on services in a service group.
- Selecting subscribed resources to deploy to services in a service group.
- Removing resources that are selected for deployment on services in a service group.

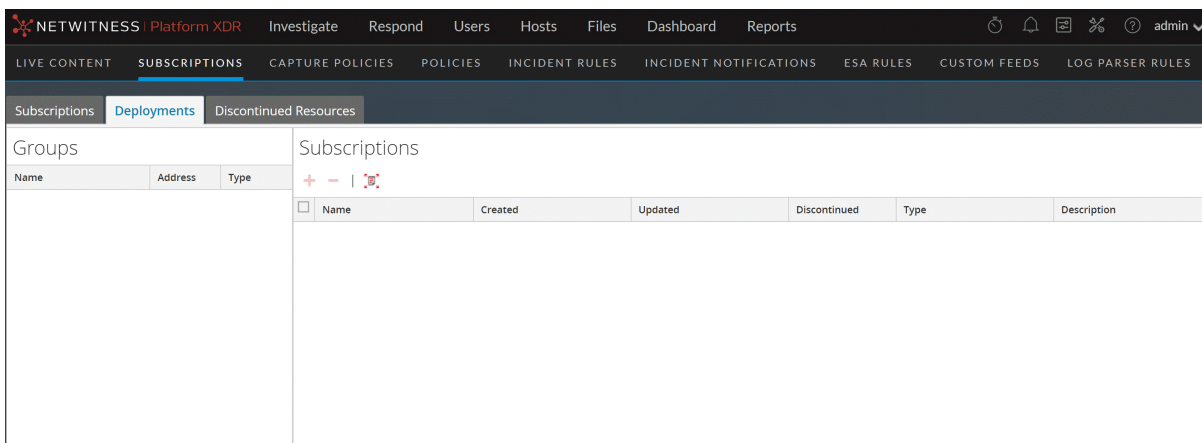
The resources listed here are not deployed immediately after adding to a service group. Instead the subscribed resources are pushed to the services when NetWitness synchronizes with NetWitness Live. The synchronization schedule is configured in the Live Configuration panel. Additionally, you can synchronize immediately in the  **(Configure) > Subscriptions > Deployments** tab.

Likewise, resources deleted from the Deployments panel are not deleted from service where they have been deployed. To delete resources from services, delete them in the Live Resource View.

The required permission to access this view is **Manage Live Resources**.

### To access this view:

1. Go to  **(Configure) > Subscriptions**.  
The **Subscriptions** tab is displayed.
2. Click the **Deployments** tab.



The Deployments tab has two panels: **Groups** and **Subscriptions**.

### Groups Panel







The Groups panel is a static display of configured service groups that were created in the Administration Services view. Selecting a group in the Groups panel populates the Subscriptions panel with a list of subscriptions that are selected for deployment on the services in the service group.

Feature	Description
<b>Name</b>	Displays the service group name. Clicking the plus sign displays a nested list of services in the group.
<b>Address</b>	Displays the IP address of each service in the group.

Feature	Description
<b>Type</b>	Displays the type of service.

*Subscriptions Panel*

The following table describes the features in the Subscriptions panel.

Feature	Description
	Click  to open a dialog that lists subscriptions that were added in the Live Search view or in the Live Resource view and are available for deployment.
	Click  to delete the selected subscriptions from the deployment list for service group.
	Click  to synchronize your resources to the latest versions available on Live.
<b>Name</b>	Displays name of the resource.
<b>Created</b>	Displays date and time that the resource was created.
<b>Updated</b>	Displays date and time that the resource was last updated.
<b>Type</b>	Displays type of resource.
<b>Description</b>	Displays description of the resource.

## Subscriptions Tab

Subscriptions are NetWitness Live resources to which you subscribed in the Live Search view or Live Resource view. When you subscribe to a resource, you agree to receive updates on a regular basis from NetWitness Live. The choices made in the Live Configuration panel determine the synchronization frequency and also whether you receive update notifications through email. In addition, if you don't want to wait for the next update, you can force an immediate synchronization.

The Subscriptions tab provides a way to manage subscriptions. Each resource to which NetWitness is subscribed is listed in this tab.

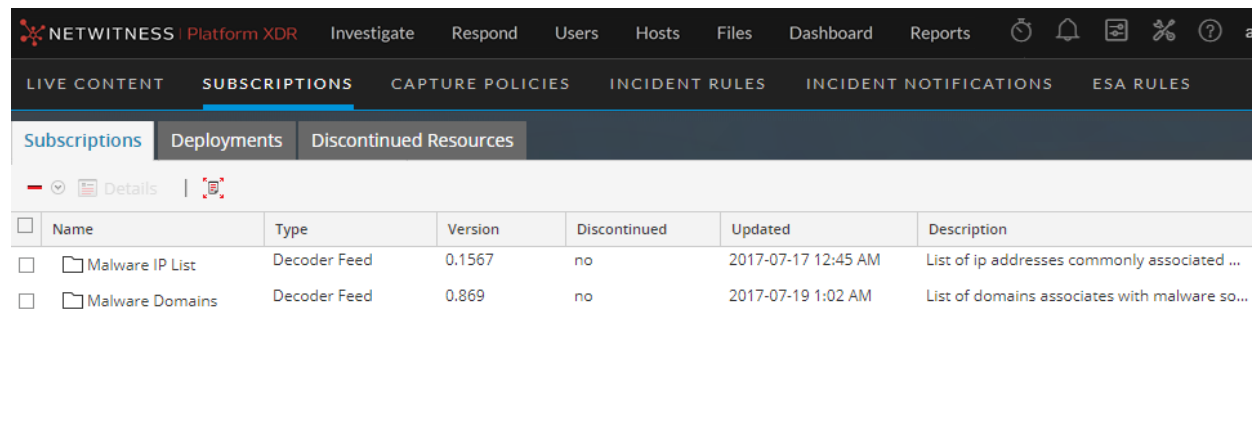
In the Subscriptions tab, you can:

- View all resources to which this NetWitness instance is subscribed.
- Open a detailed view of a subscription in the Live Resource View.
- Delete a subscription.

**Note:** Subscribing to a resource does not deploy the resource to any services. To deploy one or more subscribed resources, go to the Deployments tab. To deploy a single resource manually, use the Deploy option in the Resource View.

The required permission to access this view is **Manage Live Resources**.

To access this view, in the main menu, select  (Configure) > **Subscriptions**. The Subscriptions tab is displayed.






Name	Type	Version	Discontinued	Updated	Description
<input type="checkbox"/> Malware IP List	Decoder Feed	0.1567	no	2017-07-17 12:45 AM	List of ip addresses commonly associated ...
<input type="checkbox"/> Malware Domains	Decoder Feed	0.869	no	2017-07-19 1:02 AM	List of domains associates with malware so...

The **Subscriptions** tab has a toolbar and a grid.


### Toolbar

This table describes the options available in the toolbar.

Feature	Description
	Deletes the selected subscriptions.
 Details	Displays the details of a single subscribed resource in the Resource View.

Feature	Description
	Check the Live Server for the latest discontinued resources.

*Grid*

Column	Description
	Selects subscribed resources to view in detail or delete. You can view details for a single resource. You can delete one or more resources from the subscribed resources, in effect unsubscribing.
<b>Name</b>	Displays name of the subscribed resource.
<b>Type</b>	Displays type of subscribed resource.
<b>Version</b>	Displays version of the subscribed resource.
<b>Discontinued</b>	Indicates the status of the discontinued resources for the subscribed resource. <b>Yes</b> - Resource is discontinued. <b>No</b> - Resource is not discontinued. -- - The Live Server is not checked for the discontinued resources.
<b>Updated</b>	Displays date and time when the subscribed resource was last updated.
<b>Description</b>	Displays description of the subscribed resource.

## Discontinued Resources Tab

The Discontinued Resources tab provides a user interface in the Live Configure view:

- Scan the services for the discontinued resources.
- Remove the discontinued resources from any service or service group.

**Note:** Discontinued content still appears. With discontinued content there just won't be any updates, and users won't see these items when they search in Live, unless they check the **Include Discontinued Resources** box while searching.

In the RSA Content space on NetWitness Community, you can view the complete, up-to-date list of discontinued resources ([Discontinued Content](#)). For each resource, there is a description of why it was discontinued. Use these details to determine whether or not to remove a discontinued resource from your installation. .

The required permission to access this view is **Manage Live Resources**.

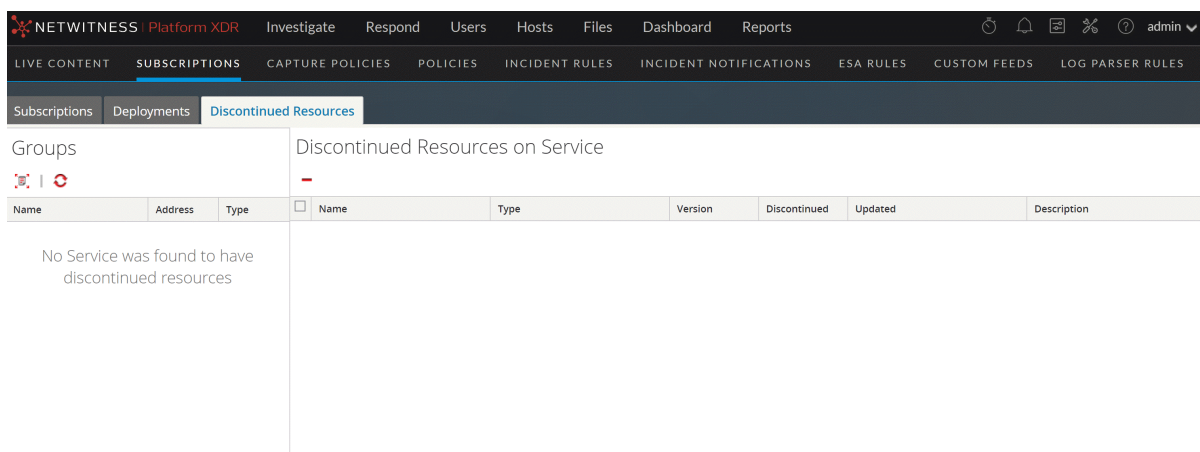
### To access this view:

1. Go to  **(Configure) > Subscriptions**.

The **Subscriptions** tab is displayed.

2. Click the **Discontinued Resources** tab.



The Discontinued Resources tab is displayed.



The Discontinued tab has two panels: Groups and Discontinued Resources on Service.


### Groups Panel

The Groups panel is a static display of configured service groups that were created in the Admin Services view. Selecting a group in the Groups panel populates the Discontinued Resources panel with a list of discontinued resources which are deployed on the selected service or service group.

Feature	Description
	Click the button to scan the services for a discontinued resource.
	Displays the current status of the discontinued resources on a service. <b>Note:</b> The status of a service may change while the services are being scanned.
<b>Name</b>	Displays service group name. Clicking the plus sign displays a nested list of services in the group.
<b>Address</b>	Displays IP address of each service in the group.
<b>Type</b>	Displays type of service.

*Discontinued Resources on Service Panel*

The following table describes the features in the Discontinued Resources on Service panel.

Feature	Description
	Click the button to delete the selected resources from the service or service group.
<b>Name</b>	This is the name of the resource.
<b>Type</b>	This is the type of resource.
<b>Version</b>	Version of the discontinued resource.
<b>Discontinued</b>	Indicates the status of the discontinued resources for the subscribed resource. <b>Yes</b> - The resource is discontinued. <b>No</b> - The resource is not discontinued. -- - The Live Server is not checked for the discontinued resources.
<b>Updated</b>	Displays date and time that the resource was last updated.
<b>Description</b>	Displays description of the resource.



## Live Feeds View

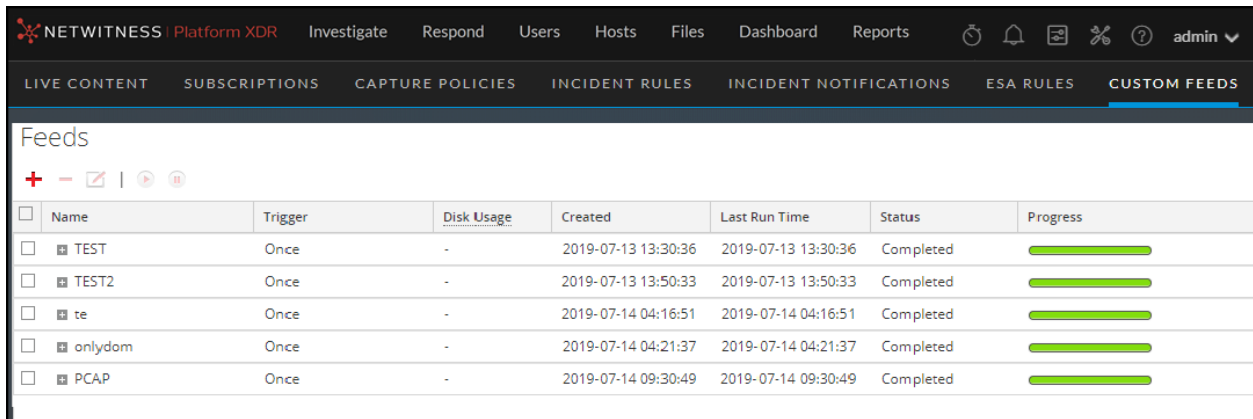
Use the Live Feeds View to:

- Create custom feeds.
- Create identity feeds.
- Edit feeds.

The required role to access this view is **Manage Devices**.

To access this view, navigate to  **(Configure) > Custom Feeds**.

This is an example of the Feeds view.


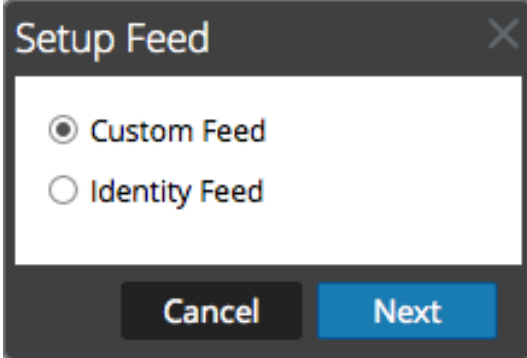






<input type="checkbox"/>	Name	Trigger	Disk Usage	Created	Last Run Time	Status	Progress
<input type="checkbox"/>	TEST	Once	-	2019-07-13 13:30:36	2019-07-13 13:30:36	Completed	<div style="width: 100%;"></div>
<input type="checkbox"/>	TEST2	Once	-	2019-07-13 13:50:33	2019-07-13 13:50:33	Completed	<div style="width: 100%;"></div>
<input type="checkbox"/>	te	Once	-	2019-07-14 04:16:51	2019-07-14 04:16:51	Completed	<div style="width: 100%;"></div>
<input type="checkbox"/>	onlydom	Once	-	2019-07-14 04:21:37	2019-07-14 04:21:37	Completed	<div style="width: 100%;"></div>
<input type="checkbox"/>	PCAP	Once	-	2019-07-14 09:30:49	2019-07-14 09:30:49	Completed	<div style="width: 100%;"></div>

The **Feeds** tab has a toolbar and a grid.


### Toolbar

This table describes the options in the toolbar.

Feature	Description
	<p>Initiates the creation of a custom or identify feed by displaying the <b>Setup Feed</b> dialog is displayed.</p>  <ul style="list-style-type: none"> <li>• Custom Feed opens the <b>Configure a Custom Feed</b> wizard.</li> <li>• Identity Feed opens the <b>Configure Identity Feeds</b> wizard.</li> </ul>
	Deletes the feed that you selected.
	Opens the Configure Custom Feed or Configure Identity Feed wizard for the feed that you selected (see <a href="#">Editing a Feed</a> ).
	Start or resume data feed.
	Stop or pause data feed.

### Feeds Grid

This table describes the columns in the grid.

Column	Description
	Selects a feed.
<b>Name</b>	<p>Name of the feed.</p> <div style="border: 1px solid green; padding: 2px; margin-top: 5px;"> <p><b>Note:</b> You can now use special characters to define the name of the custom feed.</p> </div>
<b>Trigger</b>	Displays how often the feed runs which is determined by what you defined in <b>Feed Task Type</b> when the feed was created.
<b>Created</b>	Displays date and time when the feed was created.
<b>Disk Usage</b>	Displays the MongoDB storage size used by the TAXII feed.
<b>Last Run Time</b>	Displays date and time when the feed was last run.
<b>Status</b>	The status of the feed.
<b>Progress</b>	Progress bar.


## Live Resource View

The Live Resource View shows a detailed view of a selected resource, and has the following options:

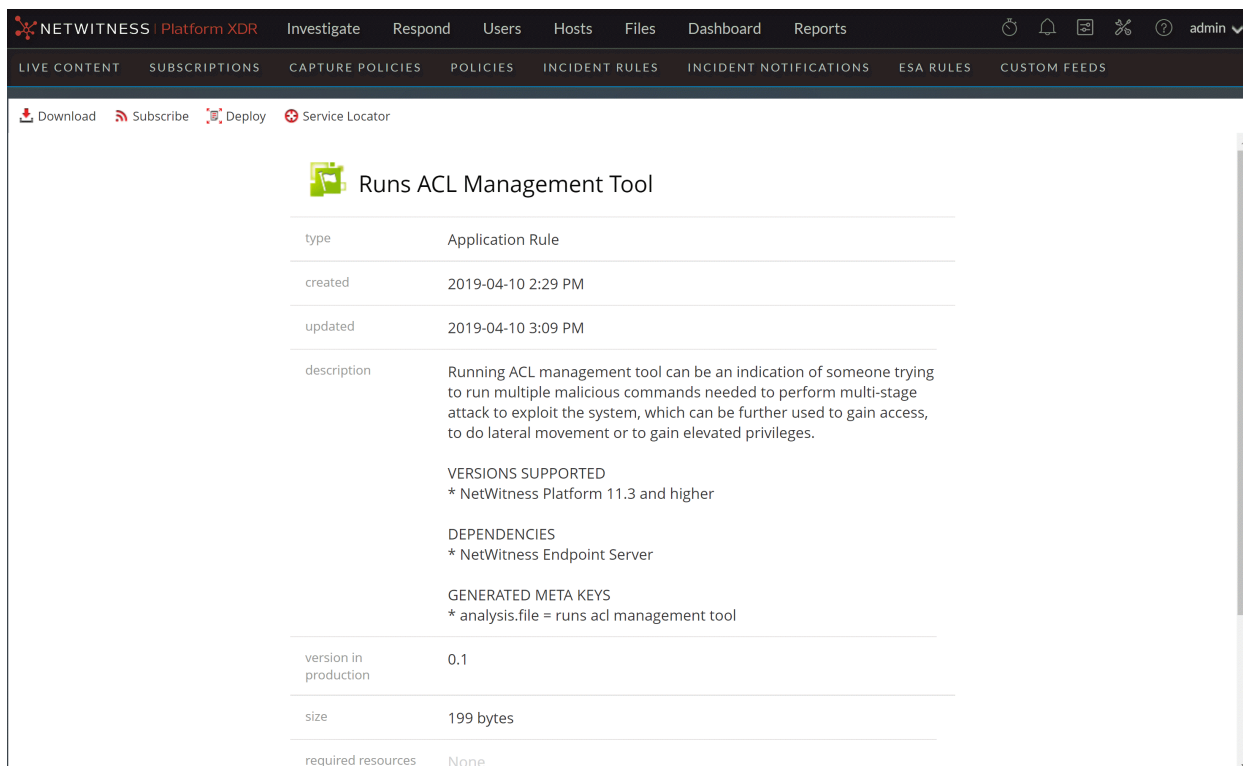
- Download the resource.
- Subscribe or unsubscribe the resource.
- Deploy the resource to services.
- Locate services on which the resource is deployed and remove the resource from services.

The required permission to access this view is View Live Resource Details.

To access this view, do one of the following:

1. Go to  (Configure) > LIVE CONTENT > Search Criteria.
2. In the Live Search view, **Detailed Results**, click the resource type icon or the resource name.
3. In the Live Search view, **Grid Results**, double-click a resource or select a resource and click **Details**.

This is an example of the Resource view.







The screenshot shows the NetWitness Platform XDR interface. The top navigation bar includes 'Investigate', 'Respond', 'Users', 'Hosts', 'Files', 'Dashboard', and 'Reports'. Below this is a secondary navigation bar with 'LIVE CONTENT', 'SUBSCRIPTIONS', 'CAPTURE POLICIES', 'POLICIES', 'INCIDENT RULES', 'INCIDENT NOTIFICATIONS', 'ESA RULES', and 'CUSTOM FEEDS'. The main content area features a toolbar with 'Download', 'Subscribe', 'Deploy', and 'Service Locator' icons. The resource details for 'Runs ACL Management Tool' are displayed as follows:

type	Application Rule
created	2019-04-10 2:29 PM
updated	2019-04-10 3:09 PM
description	<p>Running ACL management tool can be an indication of someone trying to run multiple malicious commands needed to perform multi-stage attack to exploit the system, which can be further used to gain access, to do lateral movement or to gain elevated privileges.</p> <p>VERSIONS SUPPORTED * NetWitness Platform 11.3 and higher</p> <p>DEPENDENCIES * NetWitness Endpoint Server</p> <p>GENERATED META KEYS * analysis.file = runs acl management tool</p>
version in production	0.1
size	199 bytes
required resources	None

The Live Resource View has a detailed view of a single resource and a toolbar.


## Resource Details

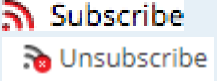
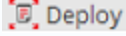
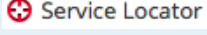
The following table describes the elements in the Resource Details section.

Feature	Description
<b>Resource Type Icon</b>	A graphic representation of the resource type, for example  .
<b>Name</b>	The name of the resource, for example, <b>fingerprint_office_lua</b> .
<b>Type</b>	The type of resource, for example, <b>RSA Lua Parser</b> .
<b>Created</b>	The date the resource was created, for example, <b>2013-09-15 02:16 PM</b> .
<b>Updated</b>	The date the resource was last updated, for example, <b>2013-09-15 02:16 PM</b>
<b>Description</b>	The description of the resource, for example, <b>Identifies Microsoft Office 95, 2007 Word, Excel, and PowerPoint documents</b> .
<b>Version in production</b>	The version of the resource, for example, <b>0.1</b> .
<b>Size</b>	The size of the resource, for example, <b>9.079 KB</b> .
<b>Required Resources</b>	A list of resources on which this resource depends, for example, <b>NetWitness Lua Library</b> . Clicking a resource replaces the currently displayed details with the details of the one you clicked.
<b>Tagged as</b> 	The tags that apply to the resource. In the example, the tags are <b>featured, informational</b> . Clicking a tag opens the Live Search View with the search narrowed to match resources with that tag.
<b>Required Meta Keys</b>	The meta keys  that apply to the resource. In the example, there are no meta keys required. Clicking a meta key opens the Live Search View with the search narrowed to match resources with that meta key.
<b>Generates Meta Values</b>	The meta values  that the resource generates. In the example, there are no meta values generated. Clicking a meta value opens the Live Search View with the search narrowed to match resources with that meta value.
<b>Permissions</b>	The permissions required for the resource.

### Resource View Toolbar

This table describes the Live Resource view toolbar options.

Feature	Icon	Description
<b>Download</b>	 <b>Download</b>	This option downloads the resource currently displayed in the Resource View.

Feature	Icon	Description
<b>Subscribe or Unsubscribe</b>		<p>This option subscribes to or unsubscribes from the resource currently displayed in the Resource View.</p> <ul style="list-style-type: none"> <li>Clicking <b>Subscribe</b> opens a dialog notifying that you are agreeing to receive notification when the selected resources are updated. You can cancel or click <b>OK</b>.</li> <li>Clicking <b>Unsubscribe</b> asks for confirmation that you want to stop receiving notification when the selected resources are updated. You can then choose to cancel or you can click <b>Unsubscribe</b> or <b>Unsubscribe and Remove</b>, which also removes the resource from services on which it is deployed.</li> </ul>
<b>Deploy</b>		<p>This option provides a way to deploy the resource currently displayed in the Resource View. Clicking <b>Deploy</b> opens the Manual Resource Deployment dialog.</p>
<b>Service Locator</b>		<p>This option displays a list of services on which the currently displayed resource is deployed. You can remove the resource from all services or selected services.</p>

## Live Search View

The Live Search view provides the ability to browse the configured Live CMS for resources. Once matching resources are found, you can view details, subscribe to resources, and deploy resources to services and service groups.

This is an example of the Search view.

The screenshot displays the NetWitness Platform XDR interface. At the top, there is a navigation bar with tabs for Investigate, Respond, Users, Hosts, Files, Dashboard, and Reports. Below this is a secondary navigation bar with various menu items like LIVE CONTENT, SUBSCRIPTIONS, CAPTURE POLICIES, etc. The main area is split into two panels. The left panel, titled 'Search Criteria', contains several input fields and dropdown menus for filtering search results. The right panel, titled 'Matching Resources', displays a table of search results with columns for 'Subscribed', 'Name', 'Created', 'Updated', 'Type', and 'Description'. A 'Search' button is located at the bottom of the search criteria panel.

The Live Search view has a panel for specifying search criteria and a panel that displays matching resources. The Search Criteria panel is collapsible to provide more width for viewing the Matching Resources panel.

### Search Criteria Panel

This is an example of the Search Criteria panel.

**Search Criteria**

Keywords

Category  
 FEATURED  
 THREAT  
 IDENTITY  
 ASSURANCE  
 OPERATIONS

Resource Types

Medium

Required Meta Keys

Generated Meta Values

Resource Created Date:  
 Start Date  End Date



Resource Modified Date:

The following table provides descriptions of the Search Criteria panel features.

Feature	Description
<b>Keyword(s)</b>	Enter a keyword or keywords to browse for resources that have the keyword in the resource name or the resource description. You can use wildcards when you enter a keyword.
<b>Category</b>	The categories mirror the hierarchical Investigation Model that NetWitness uses to organize resources. The purpose of the Investigation model is to deliver an accurate path to information security incident response. For more information, see the <a href="#">Investigation Model</a> topic in the <a href="#">NetWitness Content space</a> on NetWitness Community.

Feature	Description
<b>Resource Types</b>	<p>Select resources types from the drop-down list to filter resources by type of resource. Possible values are:</p> <ul style="list-style-type: none"><li>• Advanced Analytics (Warehouse)</li><li>• Application Rule</li><li>• Bundle</li><li>• Correlation Rule</li><li>• Event Stream Analysis Rule</li><li>• Feed</li><li>• FlexParser</li><li>• Investigation Column Group</li><li>• Investigation Meta Group</li><li>• Investigation Profile</li><li>• Log Collector</li><li>• Log Device</li><li>• Lua Parser</li><li>• Malware Rules</li><li>• NetWitness List</li><li>• NetWitness Report</li><li>• NetWitness Rule</li><li>• (Version 11.5 and later) Health and Wellness Dashboards</li><li>• (Version 11.5 and later) Health and Wellness Monitors</li></ul> <div data-bbox="418 1352 1414 1430" style="border: 1px solid green; padding: 5px;"><p><b>Note:</b> Some rules that have been deployed to an earlier version of NetWitness may not deploy or execute on NetWitness 11.x. For more information, see the <a href="#">Troubleshooting Live Services</a>.</p></div>
<b>Medium</b>	<p>Select one or more mediums from the drop-down list to search for content based on the meta data source.</p> <p>Available values for medium are as follows:</p> <ul style="list-style-type: none"><li>• <b>endpoint:</b> for NetWitness 11.3 and later): applied to content that uses meta derived from endpoint agent and endpoint server data</li><li>• <b>log:</b> applied to content that uses meta derived from log data</li><li>• <b>packet:</b> applied to content that uses meta derived from network packets</li><li>• <b>log and packet:</b> applied to content that correlates meta derived across log and packet data</li></ul>



Feature	Description
<b>Tags</b>	Select meta tags from the drop-down list to browse based on how the meta is tagged. For example, to browse resources for a Log Decoder, select the <b>netwitness for logs</b> tag. Alternatively, you can click a tag in the Matching Resources panel to insert that tag in this field.
<b>Required Meta Key(s)</b>	Enter a specific meta key; for example, <b>threat.source</b> . Alternatively, you can click a meta key in the Matching Resources panel to insert that tag in this field.
<b>Generated Meta Value(s)</b>	Enter a generated meta value; for example, <b>netwitness</b> . Alternatively, you can click a generated meta key in the Matching Resources panel to insert that tag in this field.
<b>Research Created Date</b>	Specify a date range during which resources were created. For example, to browse resources that were created between January 1 and January 4, you select January 1 as the start date and January 4 as the end date. You must enter dates in mm/dd/yyyy format or you click  and pick dates from a calendar.
<b>Research Modified Date</b>	Specify a date range during which resources were modified. For example, to browse resources that were modified between January 1 and January 4, you select January 1 as the start date and January 4 as the end date. You must enter dates in mm/dd/yyyy format or you click  and pick dates from a calendar.
<b>Search</b>	Click <b>Search</b> to send the search request to the Live server. More specific search criteria return matching resources more quickly.
<b>Cancel</b>	Click <b>Cancel</b> to cancel the search in progress.
<b>Include Discontinued Resources</b>	Check <b>Include Discontinued Resources</b> to include the discontinued resources in the search result. For an up-to-date list of resources that have been discontinued, see the <a href="#">Discontinued Content</a> topic.


### Matching Resources Panel




The Matching Resources panel displays search results based on the selections made in the Search Criteria panel. Results are initially displayed in a grid, but you can switch between two Show Results options: Detailed or Grid.

#### *Detailed Results*

In the detailed results, you can click a tag, meta key, or resource meta value to auto fill the Search Criteria panel and pivot the search results.

The following table describes the elements in the detailed results.

Feature	Description
<b>Resource Type Icon</b>	A graphic representation of the resource type. For example  .
<b>Name</b>	The name of the resource, for example, <b>Group Management</b> . <div style="border: 1px solid green; padding: 2px; margin-top: 5px;"><b>Note:</b> <b>(Discontinued)</b> is displayed next to the resource name if a resource is discontinued.</div>
<b>Type</b>	The type of the resource, for example, <b>Rule</b> .
<b>Updated</b>	The date when the resource was last updated, for example, <b>2015-09-15 4:27 PM</b> .
<b>Version</b>	The version of the resource, for example, <b>0.1</b> .

Feature	Description
Size	The size of the resource, for example, <b>153 B</b> .
Subscribed	Subscription status: <ul style="list-style-type: none"> <li>• <b>yes</b>: This NetWitness instance is subscribed to this content resource.</li> <li>• <b>no</b>: This NetWitness instance has not subscribed to this content resource.</li> </ul>
Description	The description of the resource, for example, <b>Compliance Rule-Group Management</b> .
Tags	The tags that apply to the resource. Clicking a tag narrows the search to resources with that tag. For example,  .
Meta Keys	The meta keys that apply to the resource. Clicking a meta key narrows the search to resources with that meta key. For example,  .
Resource Meta Values	The meta values generated by the resource. Clicking a meta value narrows the search to resources that generated the meta value. For example,  .






**Grid Results**

In the grid view, you can select one or more resources and use additional options in the toolbar to view the details of a single resource, subscribe to resources, and deploy resources.


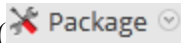
The following table describes the elements in the grid results.

Feature	Description
Subscribed	Subscription status: <ul style="list-style-type: none"> <li>• <b>yes</b>: This NetWitness instance is subscribed to this content resource.</li> <li>• <b>no</b>: This NetWitness instance has not subscribed to this content resource.</li> </ul>
Name	The name of the resource, for example, <b>Group Management</b> . <div style="border: 1px solid green; padding: 2px; margin-top: 5px;"> <b>Note:</b> The resource name is displayed in red color if it is discontinued.                     </div>
Created	The date when the resource was created, for example, <b>2015-08-12 3:11 PM</b> .
Updated	The date when the resource was last updated, for example, <b>2015-09-15 4:27 PM</b> .
Type	The type of the resource, for example, <b>Rule</b> .
Discontinued	The status of the discontinued resources: <ul style="list-style-type: none"> <li>• <b>yes</b>: The resource that matches the search criteria is discontinued</li> <li>• <b>no</b>: The resource is not discontinued</li> <li>• <b>--</b>: The Live Server is not checked for the discontinued resources</li> </ul>
Description	The description of the resource, for example, <b>Compliance Rule-Group Management</b> .

**Toolbar**

Feature	Description
 Show Results	This menu offers two ways to view search results: <b>Detailed</b> and <b>Grid</b> .
 Details	This option applies to a single selected resource. Clicking <b>Details</b> opens the selected resource in the Live Resource view.
 Deploy	This option applies to one or more selected resources.
 Subscribe	This option applies to one or more selected resources. Clicking <b>Subscribe</b> opens a dialog that asks for confirmation that you want to receive notification when the selected resources are updated.
 Package	This menu offers two packaging functions for the selected resources: <ul style="list-style-type: none"> <li>• <b>Create</b>: creates a <b>resourceBundle.zip</b> file that contains the selected resources and opens a dialog in which you can either: <ul style="list-style-type: none"> <li>• open the file, or</li> <li>• save the file for subsequent deployment.</li> </ul> </li> <li>• <b>Deploy</b>: opens the Deployment Wizard, in which you can choose a <b>resourceBundle.zip</b> file and deploy it.</li> </ul>

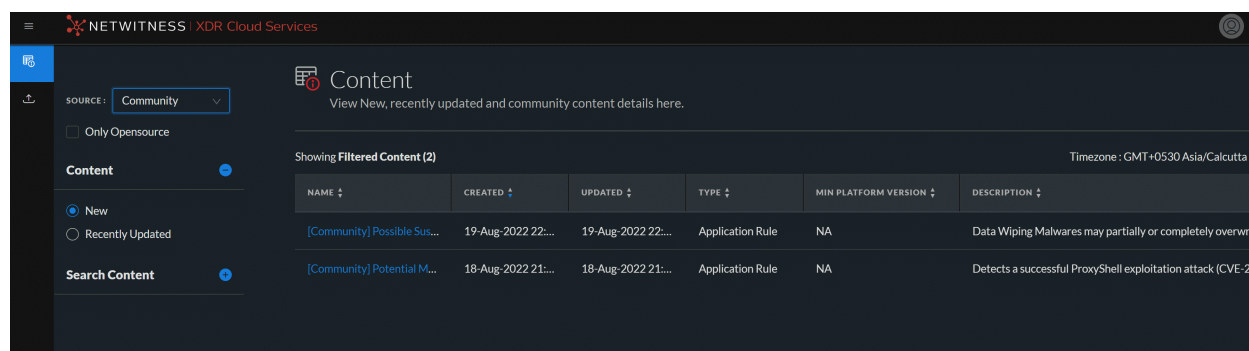
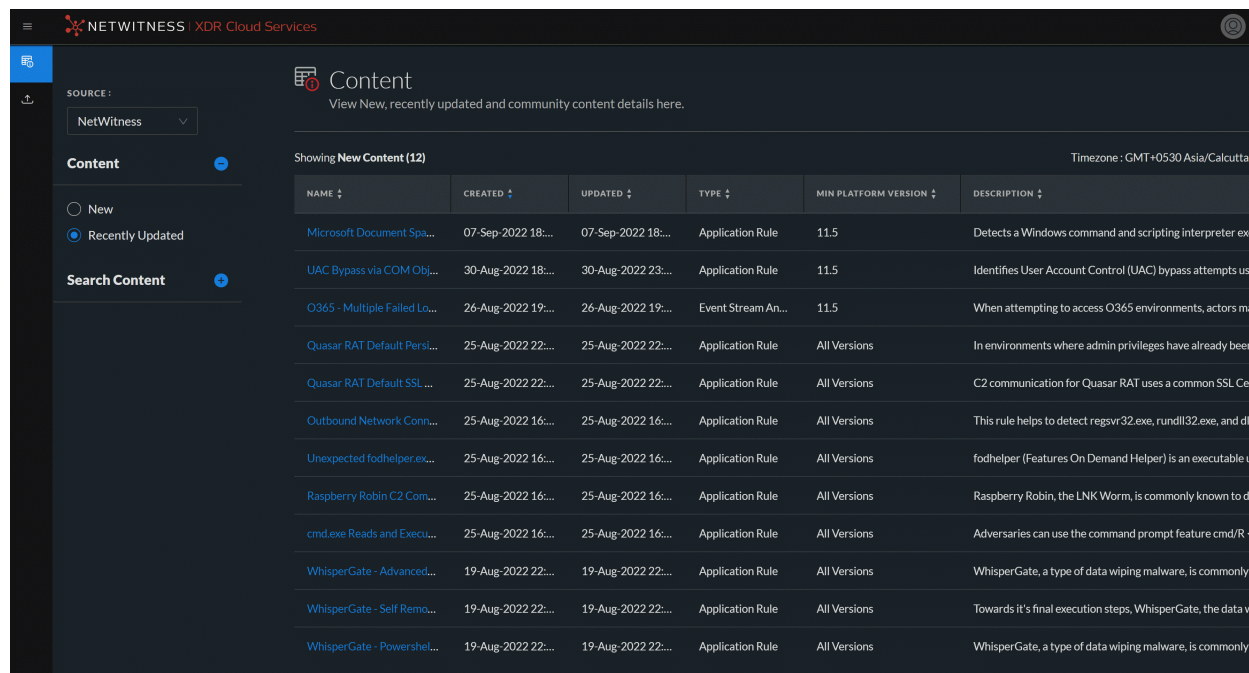
#### See Also

- For more information on Deployment () , see [Find and Deploy Live Resources](#).
- For more information on Deploying a Package () , see the [Resource Package Deployment Wizard](#).

## Live Search Content View

The Live Search Content view provides the ability to search the configured Live CMS for content. Once matching content are found, you can view the details, and download the content.

This is an example of the Search Content view.



The Live Search Content view has a panel for selecting the source and specifying search content. The matching content are displayed on the right panel.

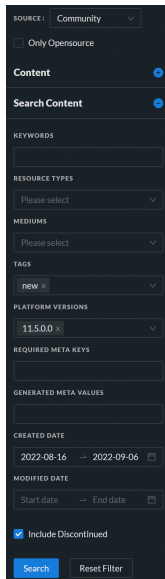
The following table provides descriptions of the Live Search Content panel features.

Feature	Description
<b>NetWitness</b>	Select NetWitness from the Source drop-down menu to search for the content that is provided by NetWitness Platform XDR Live.
<b>Community</b>	Select Community from the Source drop-down menu to search for the content collected and retrieved from third party and open source communities.

Feature	Description
<b>Only Opensource</b>	Select the Only Opensource checkbox to retrieve the content from the open-source communities.  <b>Note:</b> When the community is selected as the source, the Only Opensource option will be displayed under the Search Content Panel to select and search for open source-related content.
<b>New</b>	Select New to retrieve the content which is created in the last 21 days.
<b>Recently Updated</b>	Select Recently Updated to retrieve the content which is updated in the last 21 days.

### Search Content Panel



This is an example of the Search Content panel.



The following table provides descriptions of the Search Content panel features.

Feature	Description
<b>Keywords</b>	Enter a keyword or keywords to browse for content that have the keyword in the resource name or the resource description. You can use wildcards when you enter a keyword.

Feature	Description
<b>Resource Types</b>	<p>Select resources types from the drop-down list to filter resources by type of resource. Possible values are:</p> <ul style="list-style-type: none"><li>• Application Rule</li><li>• Feed</li><li>• Log Device</li><li>• Correlation Rule</li><li>• NetWitness Rule</li><li>• NetWitness Report</li><li>• Lua Parser</li><li>• Log Collector</li><li>• NetWitness List</li><li>• Malware Rules</li><li>• Event Stream Analysis Rule</li><li>• Advanced Analytics (Warehouse)</li><li>• Bundle</li><li>• Health and Wellness Dashboards</li><li>• Health and Wellness Monitors</li><li>• Investigate Profile</li><li>• Investigate Column Group</li><li>• Investigate Meta Group</li></ul>
<b>Mediums</b>	<p>Select one or more mediums from the drop-down list to search for content based on the meta data source.</p> <p>Available values for medium are as follows:</p> <ul style="list-style-type: none"><li>• endpoint: for 11.3 and higher): applied to content that uses meta derived from endpoint agent and endpoint server data</li><li>• log: applied to content that uses meta derived from log data</li><li>• packet: applied to content that uses meta derived from network packets</li><li>• log and packet: applied to content that correlates meta derived across log and packet data.</li></ul>
<b>Tags</b>	<p>Select meta tags from the drop-down list to browse based on how the meta is tagged. For example, to browse content for a Log Decoder, select the <b>netwitness for logs</b> tag.</p>

Feature	Description
<b>Platform Versions</b>	Select one or more platform versions from the drop-down list to search for content based on the versions. For example, <b>11.5</b> .
<b>Required Meta Keys</b>	Enter a specific meta key. For example, <b>threat.source</b> .
<b>Generated Meta Values</b>	Enter a generated meta value. For example, <b>rsa-firstwatch</b> .
<b>Created Date</b>	Specify a date range during which content were created. For example, to browse content that were created between January 1 and January 4, you select January 1 as the start date and January 4 as the end date. You must enter dates in yyyy/mm/dd format or you click  and pick dates from a calendar.
<b>Modified Date</b>	Specify a date range during which content were modified. For example, to browse content that were modified between January 1 and January 4, you select January 1 as the start date and January 4 as the end date. You must enter dates in yyyy/mm/dd format or you click  and pick dates from a calendar.
<b>Search</b>	Click <b>Search</b> to send the search request to the Live server. More specific search criteria return matching content more quickly.
<b>Reset Filter</b>	Click <b>Reset Filter</b> to reset the existing search results and displays all the content on the right panel.
<b>Include Discontinued</b>	Check <b>Include Discontinued</b> to include the discontinued content in the search result. For an up-to-date list of content that have been discontinued, see the <a href="#">Discontinued Content</a> topic.

### Search Results Panel

The Search Results panel displays search results based on the selections made in the Search Content panel.

This is an example of the Search Results panel.

The screenshot shows a 'Content' management interface with a header 'View New, recently updated and community content details here.' Below the header, it indicates 'Showing Filtered Content (877)' and 'Timezone: GMT+0530 Asia/Calcutta'. The main table has columns for NAME, CREATED, UPDATED, TYPE, MIN PLATFORM VERSION, DESCRIPTION, and DISCONTINUED. The table lists various content items such as 'RSA OSINT IP Threat Intel...', 'Logs Dashboard', 'Packet Overview Dashboard', etc.

NAME	CREATED	UPDATED	TYPE	MIN PLATFORM VERSION	DESCRIPTION	DISCONTINUED
RSA OSINT IP Threat Intel...	11-Sep-2020 01:2...	17-Jul-2022 10:01...	Feed	All Versions	This feed contains IP Address (IPv4 and IPv6) indicators that a...	No
Logs Dashboard	26-Nov-2020 16:5...	26-Nov-2020 16:5...	Not found	11.5.0.0	This dashboard provides information on various NetWitness P...	No
Packet Overview Dashboard	26-Nov-2020 16:5...	26-Nov-2020 16:5...	Not found	11.5.0.0	This dashboard provides information on NetWitness Platform ...	No
RSA OSINT Non-IP Threat I...	11-Sep-2020 01:2...	17-Jul-2022 10:01...	Feed	All Versions	This feed contains Non-IP Address, text based indicators like ...	No
Endpoint Server to Agent ...	26-Nov-2020 16:3...	26-Nov-2020 16:3...	Not found	11.5.0.0	Amount of Incoming UDP Packets Requested by Endpoint ser...	No
Decoder Capture Not Start...	26-Nov-2020 16:4...	26-Nov-2020 16:4...	Not found	11.5.0.0	Capture is not started on this Decoder service, so packet data ...	No
Debian Package Hash Mis...	06-Aug-2020 20:5...	13-Aug-2020 00:4...	Application Rule	11.5.0.0	A hash mismatch may indicate a file has been altered from its o...	No
AWS Route53 Resolver	23-Dec-2020 16:4...	23-Dec-2020 16:4...	Log Device	11.5.0.0	Log device content for event source AWS Route53 Resolver - ...	No
Cisco Umbrella	19-Mar-2021 19:3...	19-Mar-2021 19:3...	Log Device	11.5.0.0	Log device content for event source Cisco Umbrella - cisco_um...	No
Reporting Engine Available ...	26-Nov-2020 16:2...	26-Nov-2020 16:2...	Not found	11.5.0.0	Reporting Engine home directory /var/netwitness/re-server/r...	No
Contexthub Server Query ...	26-Nov-2020 16:4...	26-Nov-2020 16:4...	Not found	11.5.0.0	80% of the Contexthub Server's query response cache is in use.	No
Decoder Capture Rate Zero	26-Nov-2020 16:3...	26-Nov-2020 16:3...	Not found	11.5.0.0	Decoder is presently not capturing data.	No

The following table describes the elements in the search results panel.

Feature	Description
<b>Name</b>	The name of the content. For example, <b>Log Parser Pack</b> .
<b>Created</b>	The date when the content was created. For example, <b>04-Aug-2017 15:19:06</b> .
<b>Updated</b>	The date when the content was last updated. For example, <b>29-Sep-2020 20:27:14</b> .
<b>Type</b>	The type of the content. For example, <b>Bundle</b> .
<b>Min Platform Version</b>	Platform version that the content supports. For example, 11.5 and higher. <b>Note:</b> Min Platform Version is not applicable for Community content.
<b>Description</b>	The description of the content. For example, <b>Contains all parser files and log collection files</b> .
<b>Discontinued</b>	The status of the discontinued content: <ul style="list-style-type: none"> <li><b>Yes:</b> The content that matches the search criteria is discontinued</li> <li><b>No:</b> The content is not discontinued</li> </ul>

## Content Details Panel

In the Search Results panel, you can select any content titles to view the details in the pop-up window and download the content.

**Note:** NetWitness provides no assurance related to the quality and accuracy of the content provided by the third parties and open source communities.



This is an example of the Content Details panel.

The screenshot shows a 'Content Details' panel with the following information:

- NOTE:** The following content is collected and derived from third-party, open sources. RSA [NetWitness] at no times makes claims to the quality and/or efficacy above and beyond the attestations of the authors of the content itself.
- Title:** [Community] Malware, Malicious Code and APT Open Source YARA Rules
- TYPE:** Malware Rules
- UPDATED:** 16-Feb-2022 21:40:00
- DESCRIPTION:** The following corpus of YARA rules focus on the detection, identification, and analysis of various forms and types of malicious code & content (malware) and in some cases those threat actors/adversaries associated with their use and proliferation. These YARA rules have been collected from the open-source community and are being made available to our customers via our NetWitness Live Community capability.
- Mediums:** None
- TAGS:** malware, lateral-movement, remote-access-toolkit, threat, data-exfiltration, action-objective

At the bottom, there is a note: 'Large files may take longer time to start the download.' and buttons for 'Close' and 'Download'.

The following table describes the elements in the Content Details section.

Feature	Description
<b>Name</b>	The name of the content. For example, <b>Log Parser Pack</b> .
<b>Type</b>	The type of the content. For example, <b>Bundle</b> .
<b>Created</b>	The date when the content was created. For example, <b>04-Aug-2017 15:19:06</b> .
<b>Updated</b>	The date when the content was last updated. For example, <b>29-Sep-2020 20:27:14</b> .
<b>Description</b>	The description of the content. For example, <b>Contains all parser files and log collection files</b> .
<b>Version on Production</b>	The version of the content. For example, <b>0.5</b> .
<b>Size</b>	The size of the content. For example, <b>14.96 KB</b> .
<b>Required Resources</b>	A list of resources on which this resource depends. For example, <b>NetWitness Lua Library</b> . Clicking a resource replaces the currently displayed details with the details of the one you clicked in the pop-up window.

Feature	Description
<b>Tags</b>	The tags that apply to the content. For example, <b>threat</b> . Clicking a tag opens the Live Search Content view with the search narrowed to match content with that tag.
<b>Required Meta Keys</b>	The meta keys that apply to the content. For example, <b>Threat Category</b> . Clicking a meta key opens the Live Search Content view with the search narrowed to match content with that meta key.
<b>Generated Meta Values</b>	The meta values that the content generates. For example, <b>rsa-firstwatch</b> . Clicking a meta value opens the Live Search Content view with the search narrowed to match content with that meta value.
<b>Discontinued</b>	The status of the discontinued content: <ul style="list-style-type: none"><li data-bbox="418 657 1203 688">• <b>Yes:</b> The content that matches the search criteria is discontinued</li><li data-bbox="418 709 867 741">• <b>No:</b> The content is not discontinued</li></ul>

## Resource Package Deployment Wizard

If you have created a package of resources and saved it on a network drive, you can use the Resource Package Deployment Wizard to deploy the resources manually to a service or a service group without subscribing to the resources. NetWitness accepts packages in **.nwp** files or **.zip** files.



Deploying resources manually deploys them directly to the services without taking advantage of the powerful resource management capabilities of NetWitness.

If you want to receive notification and updates for updated resources and be able to easily remove resources from a service, you must subscribe to resources in the Live Search view and deploy the resources in the **Live Configure** view.

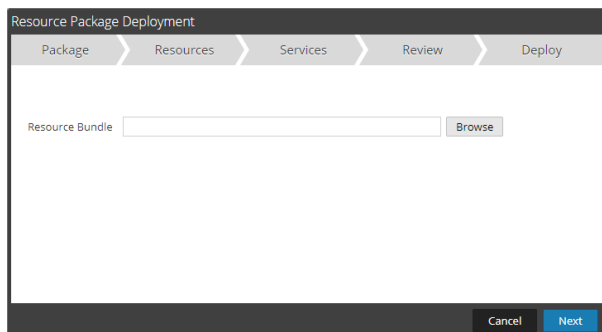
**Note:** Use NetWitness Live to create resource bundles; this is a different application that is not part of NetWitness. Selecting **Package > Create** in the **Live Search - Matching Resources** toolbar displays the Content Package Tool window. You can choose resources to include in a package and save the package as a NetWitness Package File.

The required permission to access this view is **Deploy Live Resources**.

To access this view:

1. Go to  **(Configure) > Live Content**.
2. In the **Live Search - Matching Resources** toolbar, select  **Package** > **Deploy**.

The Resource Package Deployment wizard is displayed.



### Features

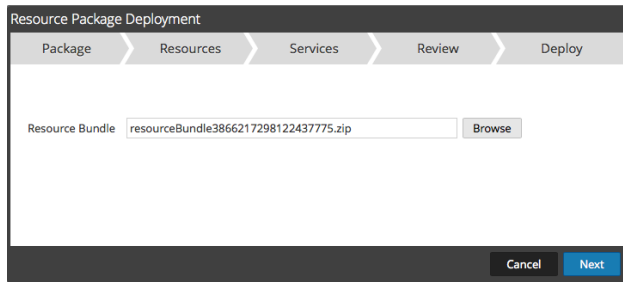
The Deployment Wizard has five tabs: **Package**, **Resources**, **Services**, **Review** and **Deploy**. Use **Close** to exit before you complete the wizard.

When you complete the wizard, NetWitness returns to the Live Resources View.

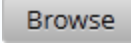
### Package Tab

You use this tab to select a resource bundle from your network in this page.

This is an example of the Package tab, with a resource bundle already selected.



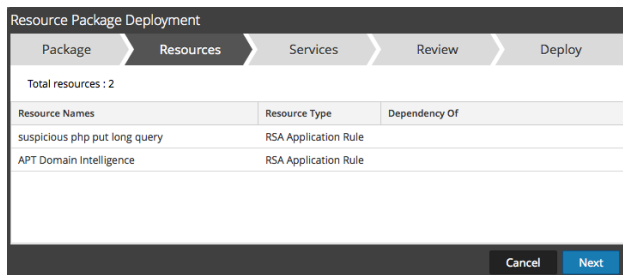
The following table describes the elements in the Package tab.

Column	Description
Resource Bundle	The input field to specify a resource bundle. You can type a path in this field or search using the  button.
Command Buttons	
Browse	This button opens a File Upload dialog in which you can browse the local file system and select a bundle.
Cancel	Cancels the deployment and closes the wizard.
Next	Displays the next tab of the wizard.

## Resources Tab

This tab displays the resources contained in the bundle.

The following figure shows an example of the Resources tab.




The following table describes elements in the Resources tab.

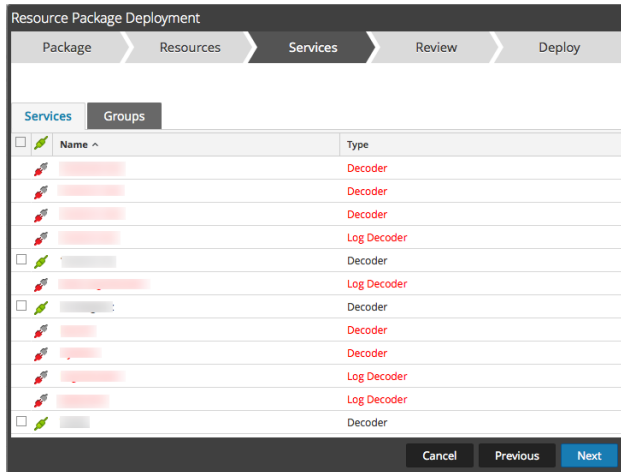
Column	Description
Resource Name	Displays the name of the resources in the bundle (for example, <b>NetWitness Lua Library</b> ).
Resource Type	Displays the resource types for the resources in the bundle (for example, <b>RSA Lua Parser</b> )
Dependency Of	Displays Resources on which the selected resource depends (for example, <b>AIM lua</b> ).

## Services Tab



You select the services on which you want to deploy the resources in the bundle.

The Services tab has two tabs, **Services** and **Groups**. These provide a list of services and service groups that are configured in the  (**Admin**) > **Services** view. The columns are a subset of the columns available in the Services view. You can select the services or the service groups on which you want to deploy the resources in the bundle.

This is an example of the Services tab.



The following table describes the elements in the Services tab.

Column	Description
<b>Services</b>	
	Selects services on which you want to deploy the content. You can select any combination of services and service groups.
Name	Displays the services in your environment on which you can deploy the content.
Host	Displays the name of the resource host.
Type	Displays the type of NetWitness service.
<b>Groups</b>	
	Selects service groups (if you have service groups defined in your environment).
Name	Displays the names of the service groups.

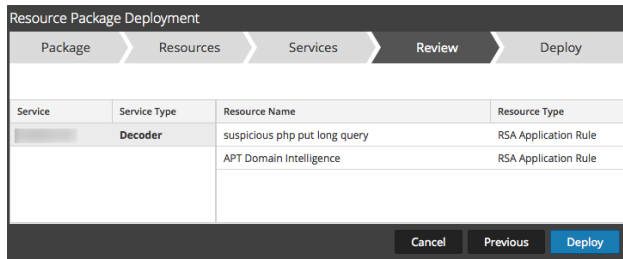
**Review Tab**

Displays the resources and services on which the resources will be deployed.

In this tab, you can do the following:

- Review the content and services before you deploy.
- Initiate the deployment of the resources.

The following figure shows an example of the Review tab.



The following table describes the elements in the Review tab.

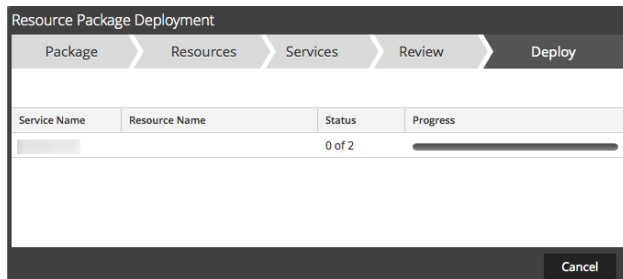
Column	Description
<b>Service Information</b>	
Service	Displays the services in your environment on which you can deploy the content.
Service Type	Displays the type of each NetWitness service (type of host or service).
<b>Resource Information</b>	
Resource Name	Displays the name of the resources you have selected (for example, <b>NetWitness Lua Library</b> ).
Resource Type	Displays the resource types for the resources you have selected (for example, <b>RSA Lua Parser</b> ).
Deploy	Initiates the deployment of the resources and displays the <b>Deploy</b> page (final page of the wizard).

### Deploy Tab

This tab allows you to do the following:

- View the progress of the job
- Cancel the job

This is an example of the Deploy tab.



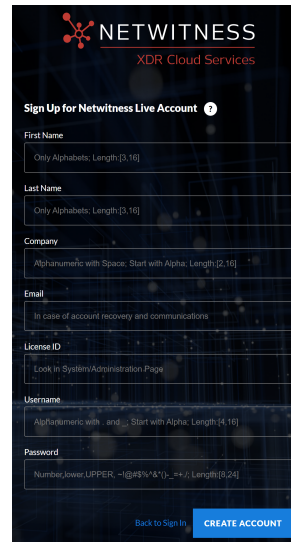
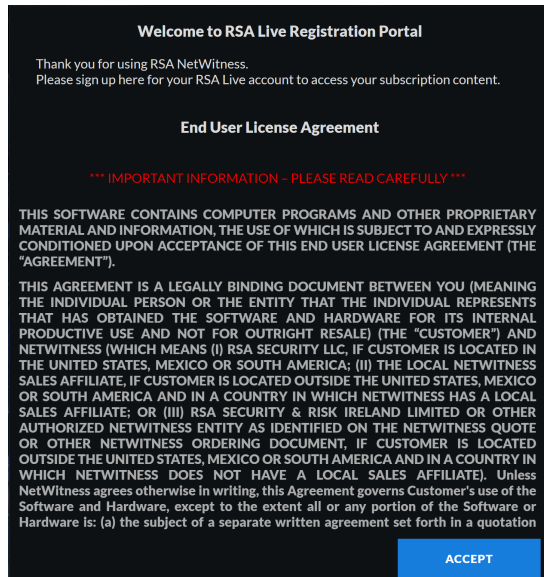
The following table describes the elements in the Deploy tab.

Feature	Description
Service Name	Name of the services to which resources are deployed.
Resource Name	Name of the resources.

Feature	Description
Status	Status of the manual deployment.
Progress	Progress of the manual deployment in a progress bar. When complete, the bar turns solid green.
<b>Command Buttons</b>	
Close	Closes the wizard.
Errors	Only displays if NetWitness encountered any errors. Click to display the errors.
Retry	Only displays if NetWitness encountered any errors. Click this button to try to deploy the resources again using the wizard.

## NetWitness Live Registration Portal

The NetWitness Live Registration Portal is a self-service wizard in which customers can set up a Live account and change or reset the password. A Live account is required to get access to the feeds, parsers, rules, and other content in NetWitness Live library. To access the portal, go to the following URL: <https://live.netwitness.com/registration>.




Click **Sign Up For Live**. The License Agreement page is displayed, once you agree to the Terms and Conditions, click **Accept**: the fields for setting up an account are displayed. These include Contact Information, and License ID.

The following table lists the contact information section fields and its descriptions:


Parameter	Description
First Name	Your first name.
Last Name	Your last name.
Company	The name of your company.
Email	The email address where you want to receive notifications related to the Live account.




Parameter	Description
License ID	<p>This is the License ID on the  (Admin) &gt; <b>System</b> &gt; <b>Info</b> page.</p> <div data-bbox="699 443 956 747" style="border: 1px solid yellow; padding: 5px;"><p><b>Caution:</b> The license ID on the NetWitness must be valid and must be registered on the Flexera Server. If not, contact NetWitness Customer Support.</p></div>
Username	<p>The username used to sign in to Cloud Services Live account. The username must contain a minimum of four characters and a maximum of 16 characters.</p>
Password	<p>The password for the Cloud Services Live account. The password must contain minimum of eight characters and the maximum length is 24, with at least one uppercase, one lowercase, one number, and one special character.</p>

## NetWitness Feedback and Data Sharing

The Live Feedback Activity Log enables you to download the usage data required for Live Feedback. After you download the Live Feedback data, you can then upload it to share with NetWitness.

The settings for these features are available in  (Admin) > System > Live Services view, in the Additional Live Services section.

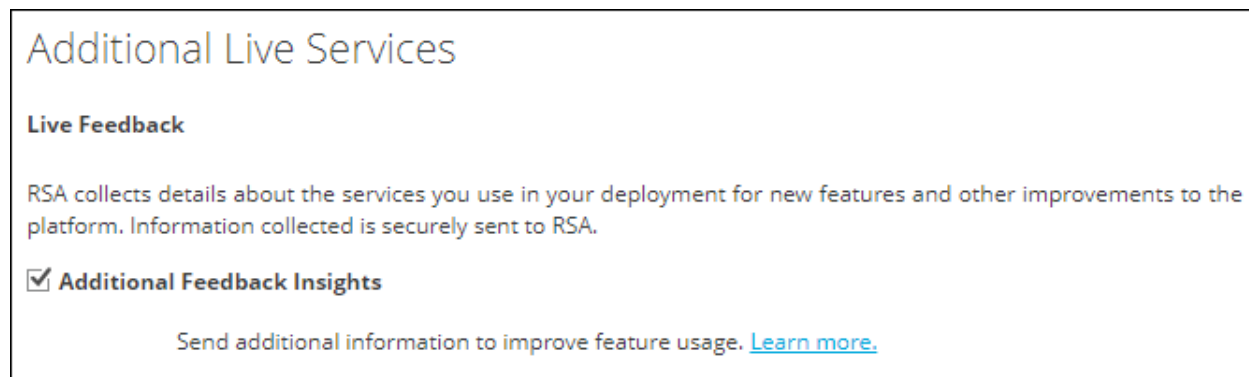
### Additional Live Services

Participation in the Additional Live Services is configured in the  (Admin) > System > Live Services view.

### Live Feedback

**Note:** For NetWitness 11.4.1 and later, this section in the UI has been removed. As of 11.4.1, NetWitness has created the Customer Experience Improvement Program. For details, see "Configure the Customer Experience Improvement Program" in the *NetWitness System Configuration Guide*.

Live Feedback is intended to help improve NetWitness.



Additional Live Services

**Live Feedback**

RSA collects details about the services you use in your deployment for new features and other improvements to the platform. Information collected is securely sent to RSA.

**Additional Feedback Insights**

Send additional information to improve feature usage. [Learn more.](#)

Once you set up and configure a Live account, usage data is automatically shared with NetWitness and is protected in accordance with the applicable license agreement. All such data shall be anonymized and shall not have any Personally Identifiable Information.

Before data is sent to NetWitness, all Personally Identifiable Information is removed. Thus, only anonymous usage data gets transferred to NetWitness.

For more information, see the "Live Feedback Overview" topic in the *System Configuration Guide*.

### File Reputation

File Reputation service provides instant access to the latest signatures using the RSA Live feed so data is more relevant, with fewer false positives. With this service, users always have reliable data about the reputation of files in their NetWitness Endpoint system. In addition to the whitelisting service, it provides blacklisting information as well.

### File Reputation

Enable   **File Reputation**    Not Connected

This option is used to view reputation status of files. The File Hash information from NetWitness Platform is sent to RSA Live to get the reputation status. Reputation status is leveraged by analysts during investigation of files.[Learn more.](#)

## Troubleshooting Live Services

This section provides troubleshooting instructions for issues faced when using the Live Services module in NetWitness.

### Some Rules Are Invalid for Version 11.x

The rules "NetWitness Incident Management - Alert Details" and "NetWitness Incident Management - Incident Summary" are not valid for NetWitness version 11.x. Do not deploy these rules to an 11.x system.

**Note:** Rules are updated frequently, and the documentation for them is available in the Content space on NetWitness Community. For the latest information on Rules, see [RSA NetWitness Rules](#).


### OutOfMemoryError on Context Hub Server

You may encounter an OutOfMemoryError on Context Hub server, and the service becomes unresponsive.

If there are any TAXII feeds configured, Health and Wellness raises alerts when the available heap memory of Context Hub server is critically low. If the status of Context Hub server is Unhealthy because of low memory, perform the following steps:

1. Make sure that the feeds **Start Date** is within 180 days.
2. Check if any TAXII feed is consuming too much disk space. A TAXII feed can consume maximum of 300 MB. If it consumes more disk space, you must reduce the value in the **Remove STIX data older than** field under **Advanced Options** in the **Custom Feed Creation Wizard** when you edit a TAXII feeds.

**Note:** If the issue still persists, you must execute step 3.

3. To decrease the number of parallel threads available for processing STIX:
  - a. Go to  (Admin) > Services > Context Hub service > View > Explore.
  - b. In the tree panel, navigate to **enrichment/stix/ config**.
  - c. In the right panel, set the **stix-query-scheduler-pool-size** field value to 2. By default the value is 5. This setting controls how many number of threads are allowed to process queries for STIX data at the same time.
  - d. Set the **taxii-poll-scheduler-pool-size** field value to 2. By default the value is 5. This setting controls how many number of threads are allowed to poll TAXII servers at the same time.
  - e. Restart the Context Hub server.

### Troubleshooting Live Connect Threat Data Sharing

This section discusses troubleshooting Live Connect Threat Data Sharing.

### Query Log Retrieval Sample

To retrieve a sample of threat intelligence data sent to Live Connect, you must construct a URL by setting the following parameters:


- **sendReport**: value is **true** or **false**: true to send this report to the Live Connect server. False to just create the report for viewing. The value defaults to false.
- **hashValues**: value is **true** or **false**: true to hash the values as md5/sha256. False to show values in clear text – should use only for manual viewing. Defaults to false.
- **startDate / endDate**: Dates for time boundaries for log entries. Format: YYYY-MM-DD HH:mm:ss

The following is an example of the URL used to retrieve query logs:

```
https://<server>/admin/liveconnect/force_aggregation?startDate=2016-01-18%2000:00:00&endDate=2016-01-19%2010:10:00&sendReport=false&hashValues=true
```

### System Logging: Debug

#### To access debug information:

1. Go to  (Admin) > System > System Logging.
2. Select the **Settings** tab.
3. In the Package Configuration section, select **com > netwitness > platform > server > liveconnect > service (DEBUG)**.

The screenshot shows a web-based management console for System Logging. On the left is a vertical navigation menu with the following items: Info, Updates, Licensing, Email, Global Notifications, Legacy Notifications, **System Logging** (highlighted), Global Auditing, Jobs, Live Services, URL Integration, Context Menu Actions, Investigation, HTTP Proxy Settings, NTP Settings, and Dashboard Settings. The main content area is titled "System Logging" and has three tabs: "Realtime", "Historical", and "Settings" (which is active). Below the tabs is a "Package Configuration" section containing a tree view of packages. The tree view shows folders for "Investigation", "list", "live", "liveconnect", "service (DEBUG)", and "malware". Under "service (DEBUG)", there are four sub-items: "LiveConnectClient", "LiveConnectLogAggregatorService", "LiveConnectLogParserService", and "LiveConnectLogRetrievalService". Below the tree view are configuration fields: "Package" with a text input containing "com.rsa.smc.sa.liveconnect.service", "Log Level" with a dropdown menu set to "DEBUG", and a checkbox for "Reset recursively" which is unchecked. At the bottom of this section are two buttons: "Apply" and "Reset". The footer of the console shows the user "admin", the language "English (United States)", and the time zone "GMT+00:00".

## Policy-based Centralized Content Management

This chapter covers different topics that lets you configure Policy-based Centralized Content Management.

- [About Policy-based Centralized Content Management \(CCM\)](#)
- [Enable or Disable CCM for All or Individual Services](#)
- [Manage Content Library](#)
  - [Migrate Content from Core Services to Content Library](#)
  - [Import Content to Content Library](#)
  - [Create an Application Rule](#)
  - [Clone Application Rule](#)
  - [Edit Application Rule](#)
  - [Delete Application Rule](#)
  - [View Application Rule Details](#)
  - [Create a Network Rule](#)
  - [Clone Network Rule](#)
  - [Edit Network Rule](#)
  - [Delete Network Rule](#)
  - [View Network Rule Details](#)
  - [Create an ESA Rule](#)
  - [Edit an ESA Rule](#)
  - [Delete an ESA Rule](#)
  - [Filter Content Rules](#)
- [Manage Groups](#)
  - [Create a Group](#)
  - [View a Group](#)
  - [Delete a Group](#)
  - [Edit a Group](#)
  - [Filter Groups](#)

- [Manage Policies](#)
  - [Create and Publish Policies](#)
  - [Clone a Policy](#)
  - [Delete a Policy](#)
  - [Edit a Policy](#)
  - [View a Policy](#)
  - [Enable Content for a Policy](#)
  - [Disable Content for a Policy](#)
  - [Filter Policies](#)
  - [Filter Policy Content Details](#)
  - [Merge Policy with ESA Content](#)
- [Manage ESA Datasources](#)
  - [View an ESA Datasource](#)
  - [Add an ESA Datasource](#)
  - [Edit an ESA Datasource](#)
  - [Delete an ESA Datasource](#)
- [Manage Deployments](#)
  - [View a Deployment](#)
  - [Create a Deployment](#)
  - [Edit a Deployment](#)
  - [Start a Deployment](#)
  - [Remove a Deployment](#)
  - [Stop a Deployment](#)
  - [Migrate ESA Deployments to Policies and Groups](#)
- [Appendix B: Position Tracking Information](#)
- [References](#)
  - [Content Library Tab](#)
  - [Groups Tab](#)
  - [Policies Tab](#)
  - [Data Sources Tab](#)
  - [Deployments Tab](#)
- [Appendix A: Endpoint Risk Scoring Rules](#)



- [Appendix B: Position Tracking Information](#)

## About Policy-based Centralized Content Management (CCM)

Legacy content management involves deploying and managing content in multiple places in the UI.

- **Live Content UI:** Located under the Configuration interface, this allows a “push” deployment of Live content to one or more services, but does not provide any management of content once it is deployed
- **Service Config UI:** Located under **Admin > Services > View Config**, this UI enables you to view, edit or delete content on individual services.

Policy-based Centralized Content Management (CCM) is a unified approach to find, deploy, and manage content through the entire life cycle based on policies that can be assigned to groups of devices. It is a single location to view, modify and manage the content deployed across all services in the environment.

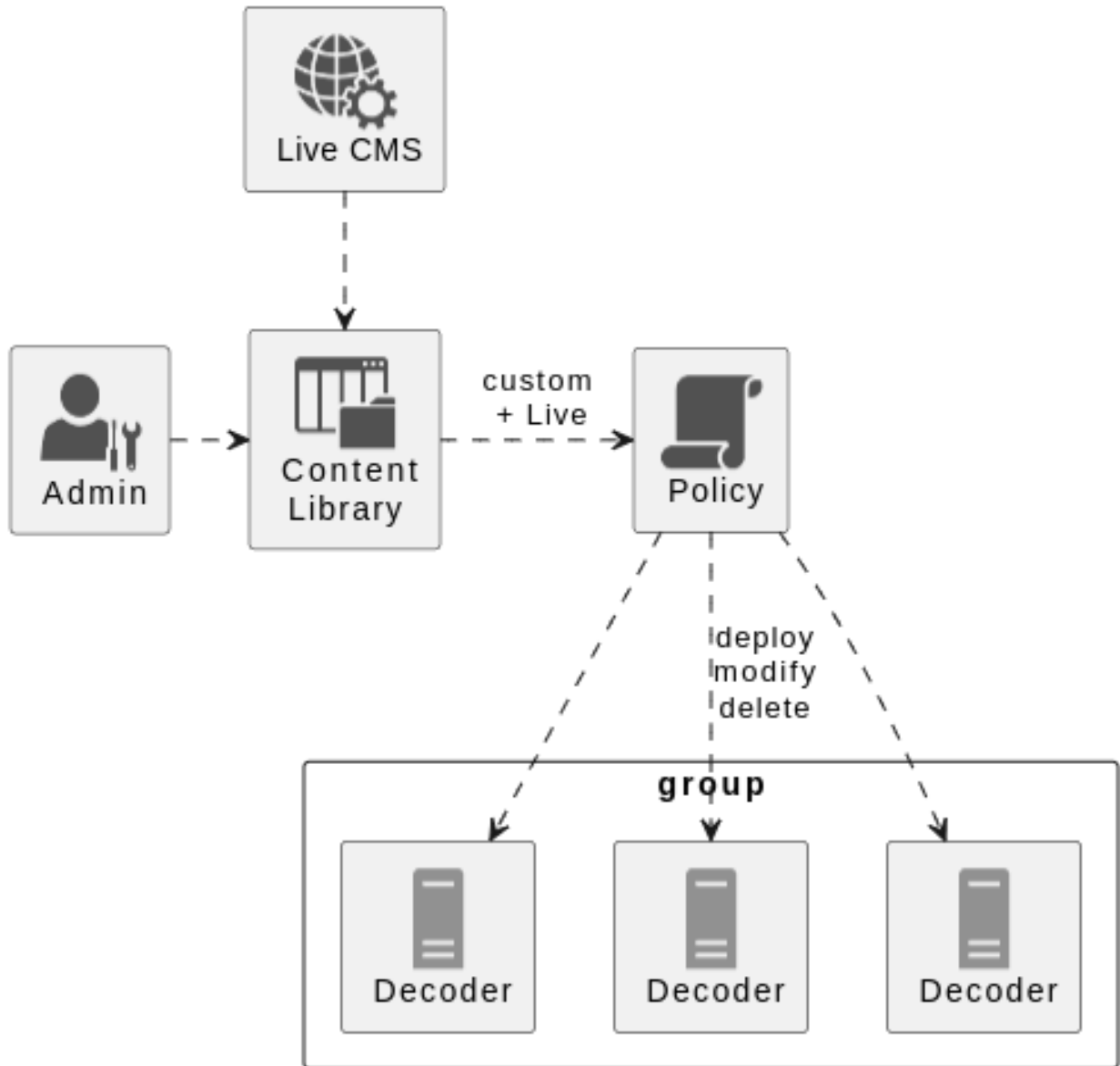
This approach consists of three elements:

- **Groups:** A collection of NetWitness services (such as Decoders, Log Decoders, and Correlation Servers etc.) to assign and manage content.
- **Content Policies:** A container of content and subscription settings used to assign and manage content within a Group.
- **Content Library:** A local repository of content which resides on the Admin Server and is used to assign content to policies. This includes both Live and Custom content.

The Content Library contains Live content (synchronized with the Live CMS) and any custom content you create or import. To deploy, remove or manage content on your services, content is assigned from the Content Library to a Content Policy. Once that content policy is assigned to a group and Published, the content changes are put into effect on the services within the group.


## Workflow

### Content Policy Flow Diagram



## Benefits

Benefits of Policy-based Centralized Content Management:

- Add or remove content without repeating the process on each service.
- Add content from RSA Live or add your custom content into a single content repository. You can add content from this repository to a policy.
- Add a new service to an existing group to automatically deploy all necessary content.
- One-click management of subscriptions and automatic updates
- Provides highly responsive and updated UI for browsing RSA Live content that can help you with the following:
  - View Live content along with your content policies and click  to add content from Live.
  - Seamlessly view Live content along with your custom content.
- Create and upload content to the Content Library easily by:
  - Importing log parsers as a zip file instead of converting to ".envision" format.
  - Cloning existing Application Rules and Network Rules.
- Switch services between legacy Content Management UI and the new Centralized Content Management via Groups and Policies using the "toggle" feature. This can prevent content being mistakenly added or modified outside of a Policy, causing an out-of-sync issue.
- Create, modify and publish policies and manage custom content in the Content Library even without an internet connection.
- Find content, policies or groups of interest easily by using the **Filtering** capability of the UI.
- Receives meta key and operator suggestions while creating Application Rule and Network Rule conditions. This eases the creation of error-free rules.
- Manage ESA content and handle multiple deployments seamlessly using Policy.
- Seamlessly view ESA Live content along with your own custom content.
- Add and manage ESA Correlation servers as part of groups.
- Manage all the data sources for the ESA Correlation servers from the **Settings > Event Stream Analysis > Data Sources** page seamlessly.

**IMPORTANT:** It is recommended not to use the Centralized Content Management and Service Config page or Live Content page simultaneously for managing the content. Using the Service Config UI to add or modify content can cause the content to become out-of-sync with the Content Policy.

**Note:** If Policy-based Centralized Content Management is enabled for a service, then the Policy-based Centralized Content Management enabled services will be disabled in Live content UI and user will not be able to manage content of these services from Service Config page as Service Config page becomes read only and no actions except 'export' can be performed from Service Config page.

## Enable or Disable CCM for All or Individual Services


Prior to 12.1 version, content of the core services could be managed simultaneously either via Policy-based Central Content Management (CCM) or Service Config page/Live content UI. Managing content in this way could cause policies to go out of sync with the actual content of the services.

From 12.1 version, by default, CCM is enabled to manage all services.

From 12.1.1 version onwards, single CCM toggle is introduced to enable or disable CCM for all 12.0+ Decoders and Log Decoders.

The toggle button is available via backend of source-server. Through the backend server, you can disable or enable Policy-based Centralized Content Management (CCM) for an individual service.

When CCM is Enabled:

- The service config page is read-only. Only **Export** button is enabled in service config page to export content.
- Content cannot be deployed to CCM enabled services through the Live Content UI.
- Content for all CCM enabled services can be managed through the Content Policies and the Content Library.
- Content subscription from CCM overrides content subscription from  (**CONFIGURE**) > **Subscriptions** page.

When CCM is Disabled:

- Content can be deployed from Live Content UI.
- The content of the service can be managed from service config page. Any changes made through the Service Config page does not reflect in the content policy.
- The service is disabled in the Policy or Group page of CCM and the policy status changes to **Partial**. The policy can be published with a disabled service. However, the policy state always remains **Partial**. Publishing a policy will affect only the services that are enabled for CCM.

**Note:** When a service, which is part of a group, is added back to CCM, the policy status changes to “Unpublished”.

## How to Enable or Disable CCM for All Services

1. Connect through SSH to NW server node.
2. Run the following commands:
  - a. `nw-shell`
  - b. `connect --service source-server`
  - c. `cd /rsa/central/service/`
  - d. `cd set-all-managed-by-legacy`
  - e. `invoke true`

Returns the message “Content of all Decoders & Log Decoders is centrally managed: No”. This message indicates that the CCM is disabled for all Decoder services.

f. `invoke false`

Returns the message “Content of all Decoders & Log Decoders is centrally managed: Yes”. This message indicates that the CCM is enabled for all Decoder services.

## How to Enable or Disable CCM for Individual Services

Follow these steps to enable or disable CCM for individual services:

1. Connect through SSH to NW server node.
2. Run the following commands:
  - a. `nw-shell`
  - b. `connect --service source-server`
  - c. `cd /rsa/central/service/`
  - d. `cd toggle-managed-by-legacy`
  - e. `invoke '<service_name>'`  
example: `invoke 'NWAPPLIANCE18845 - Log Decoder'`

## Manage Content Library

This section contains:

- [Migrate Content from Core Services to Content Library](#)
- [Import Content to Content Library](#)
- [Create an Application Rule](#)
- [Clone Application Rule](#)
- [Edit Application Rule](#)
- [Delete Application Rule](#)
- [View Application Rule Details](#)
- [Create a Network Rule](#)
- [Edit Network Rule](#)
- [Delete Network Rule](#)
- [View Network Rule Details](#)
- [Create an ESA Rule](#)
- [Edit an ESA Rule](#)
- [Delete an ESA Rule](#)
- [Filter Content Rules](#)

## Migrate Content from Core Services to Content Library

The customers who want to use Centralized Content Management, and if their content is already deployed, a migration process is required.

### Note:

- Existing Live content does not need to be exported or imported. All Live content will be available in the Content Library and will only need to be added to one or more policies and published as needed.
- When the user upgrades a Decoder or Log Decoder from 11.x, 12.0 or 12.1 version to 12.1.1 version, a back up of all the content is created automatically. Backup file will be available on Core Services' host under the following path:

For Log Decoder - `/var/netwitness/logdecoder/logdecoder_backupcontent_ccm.tar`


For Network Decoder - `/var/netwitness/decoder/decoder_backupcontent_ccm.tar`

This process includes the following steps:

- Make sure that the necessary Live content has been selected and applied to one or more Policies.
- Enable subscriptions for Live content as desired.
- Export any custom content, including Application Rules, Network Rules, Lua Parsers and Log Parsers.
- Import custom content into the Content Library.
- Apply custom content to one or more Policies.
- Create Groups to which Policies will be assigned.
- Publish Policies to their assigned Groups.

**Warning:** Initially, when a Policy is published to a Group, all the content which are not included in the policy will be removed from the services in that Group.

### To migrate Application Rules or Network Rules

1. Go to  (Admin) > Services.
2. Go to Config view of the service where application rule or network rule is deployed.
3. Click either the **Application Rule** or the **Network Rule** tab.

**Note:** The **Network Rule** tab is only available for **Network Decoder** services.

4. Select the content to migrate.
5. Click **Export** to export the selected content or click **All** to export all the content.
6. Type a file name which contains exported content and import the content to Content Library.

For details on importing content to content library, view [Import Content to Content Library](#) topic.

The following table lists the supported file types and file extensions for Application Rules and Network Rules:

Content	Supported File Types	Supported File Extensions
Application Rules	.NWR	NA
Network Rules	.NWR	NA

### To migrate Feeds, LUA Parsers, or Log Devices

The content file locations are as given below:

- Feeds content file location: /etc/netwitness/ng/feeds
- Lua Parsers content file location: /etc/netwitness/ng/parsers
- Log Devices content file location: /etc/netwitness/ng/envision/etc/devices

You can upload the files which are copied locally from these locations and import these files to Content Library.

For details on importing content to content library, view [Import Content to Content Library](#) topic.

The following table lists the supported file types and file extensions for Log Devices, LUA Parsers and Feeds:

Content	Supported File Types	Supported File Extensions
Feeds	.zip	.feed and .token
Log Devices	.envision, .zip <div style="border: 1px solid green; padding: 5px; margin-top: 5px;"> <p><b>Note:</b> The zip file should have a root folder. The root folder should contain the 'N' folders for 'N' number of content. The 'N' folder names should be the content names. The 'N' folders, will contain the respective xml files.</p> </div>	NA
LUA Parsers	.zip	.luax, .lua and .flextoken

**Note:** Any imported content will be treated as custom content. If imported content has the same name as existing Live content, then it must be renamed upon import. Custom content with the same name can be overwritten.

### To create .envision files

1. Keep all the Log Devices in a root folder in your local drive. For example, "logDevices".
2. From the command prompt, run the python script specified in the NetWitness Community portal with input argument as the path of the above folder.

**Note:** The command to run the python script is "python3 pythonscriptname.py inputArg".



3. Once you run the script, a new zip named "nw\_content\_logDevices.zip" is created. This zip file will contain all the envision files.


**IMPORTANT:** All actions except 'Export' are disabled for Application Rules, Network Rules, Feeds, LUA Parsers and Log Devices from Service Config page for all core services if the service is managed by Policy-based Centralized Content Management.

## Import Content to Content Library

Before the custom content can be used in policies, it must be imported to the Content Library.

To view the list of supported file types and file extensions for different content types, refer [Migrate Content from Core Services to Content Library](#) topic.

### To import content to Content Library

1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Depending upon the type of content to be imported, click the following tabs:
  - **Application Rule**
  - **Network Rule**
  - **LUA Parser**
  - **Feeds**
  - **Log Devices**

**Note:** Log Devices content should be converted to .envision files before importing.

5. In the respective content panel, click **Import**.
6. In the **Import** panel, click or drag the file to upload.
7. Click **Overwrite** to overwrite content. This is applicable only in case of overriding an already imported content.


**Note:** You can overwrite the content if the content name is the same as the custom content. However, overwriting is not supported if the content name is the same as existing content of the same type from the live server.

8. Select the medium types.
9. Click **Import** to complete the import process.

## Create an Application Rule

This topic describes the steps to create an application rule.

### To create a new Application Rule

1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.  
The available rules are displayed.
4. In the application rule panel, click + **Create Rule** to add an application rule.
5. In the **New Create Rule** panel, do the following:
  - Enter a unique rule name. If the name of that application rule is the same as an existing rule, an error message is displayed.
  - Enter the rule value. This is the value written to the alert meta. While creating a new rule, the rule value is defaulted with the rule name. However, you can modify the same.


**Note:** This field is applicable only for 12.1.1 version.

- Enter the condition for the rule. You can apply two types of conditions for the rule.
  - Normal mode:
    - It gives suggestions for supported metas (ip, host and so on) and operators (“=”, “Not Equal To”, “Contains”, “Exists” and so on).
    - The entered condition will be enclosed in a ‘Pill’. When you enter multiple conditions, the conditions are automatically joined by an ‘AND’ operator. On clicking the ‘AND’ operator, you can toggle between ‘AND’ and ‘OR’ operators.
  - Advanced: You can customize the conditions as a free form text.
- Select the medium to be applied for the rule.
- Enter the description for the rule.
- Select the session data to be applied for the rule.
- Select the session options to be applied for the rule.
- Enter the meta value for the alert on. This is a mandatory field.
- Click **Save** to save the new application rule.

### Clone Application Rule

This topic describes the steps to clone an application rule.

#### To clone an Application Rule

1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. The list of application rules is displayed. From the available list of rules, select the rule to be cloned.

5. Click **Clone Rule**.
6. For 12.1 version, in the Clone Rule panel, do any of the following:
  - Enter the name for cloned rule and click **Clone** to clone the rule.
  - Click **Cancel** to cancel the operation.
7. For 12.1.1 version, in the Clone Rule panel, do any of the following:
  - Enter a unique rule name. If the name of that application rule is same as an existing rule, an error message is displayed.

**Note:** The rule value cannot be modified. You can clone existing rules to generate cloned rules with different rule names but with same rule value.


- Enter the condition for the rule.
- Select the medium to be applied for the rule.
- Enter the description for the rule.
- Select the session data to be applied for the rule.
- Select the session options to be applied for the rule.
- Enter the meta value for the alert on. This is a mandatory field.
- Click **Clone** to clone the rule.
- Click **Cancel** to cancel the operation.

## Edit Application Rule

When you edit the application rule, follow these guidelines:

- You can only edit the custom rules.
- The rule name cannot be edited if the custom rule is assigned to a policy.
- If the custom rule assigned to a policy is edited, then the customer must republish the policy for the changes to take effect in the service.

### To edit an Application Rule


1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Select an application rule to edit.
5. Click **Edit Rule** to edit the application rule.

## Delete Application Rule

When you delete the application rule, follow these guidelines:

- You can delete only the custom application rules.
- You cannot delete the application rule if it is associated to a policy. You should first disassociate the application rule from the policy and then delete it.


### To delete an Application Rule

1. Go to  (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Select an application rule to delete.
5. Click **Delete** to permanently delete the selected application rule.

### View Application Rule Details

This topic describes the steps to view the application rule details.


#### To view Application Rule details

1. Go to  (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.  
The list of application rules is displayed.
4. Click a row to view details about the selected application rule in the right panel.  
The various details of the application rule are displayed.

### Create a Network Rule

This topic describes the steps to create a network rule.

#### To create a Network Rule

1. Go to  (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Click the **Network Rule** tab.
5. In the network rule panel, click + **Create Rule** to add a network rule.
6. In the **New Create Rule** panel, do the following:
  - Enter a unique rule name. If the name of that network rule is the same as an existing rule, an error message is displayed.
  - Enter the rule value. This is the value written to the alert meta. While creating a new rule, the rule value is defaulted with the rule name. However, you can modify the same.

**Note:** This field is applicable only for 12.1.1 version.

- Enter the condition for the rule. You can apply two types of conditions for the rule.
  - Normal mode:
    - It gives suggestions for supported metas (ip, host and so on) and operators (“=”, “Not Equal To”, “Contains”, “Exists” and so on).
    - The entered condition will be enclosed in a ‘Pill’. When you enter multiple conditions, the conditions are automatically joined by an ‘AND’ operator. On clicking the ‘AND’ operator, you can toggle between ‘AND’ and ‘OR’ operators.
  - Advanced: You can customize the conditions as a free form text.


**Note:** The medium is selected as **Packet** by default, and it cannot be modified.

- Enter the description for the rule.
- Select the session data to be applied for the rule.
- Select the session options to be applied for the rule.
- Click **Cancel** to cancel the operation.
- Click **Reset** to reset the data.
- Click **Save** to save the new network rule.

## Clone Network Rule

This topic describes the steps to clone an application rule.

### To clone an Application Rule

1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Click **Network Rule** tab.
5. The list of application rules is displayed. From the available list of rules, select the rule to be cloned.
6. Click **Clone Rule**.
7. For 12.1 version, in the Clone Rule panel, do any of the following:
  - Enter the name for cloned rule and click **Clone** to clone the rule.
  - Click **Cancel** to cancel the operation.
8. For 12.1.1 version, in the Clone Rule panel, do any of the following:
  - Enter a unique rule name. If the name of that network rule is same as an existing rule, an error message is displayed.

**Note:** The rule value cannot be modified. You can clone existing rules to generate cloned rules with different rule names but with same rule value.

- Enter the condition for the rule.

**Note:** The medium is selected as **Packet** by default, and it cannot be modified.


- Enter the description for the rule.
- Select the session data to be applied for the rule.
- Select the session options to be applied for the rule.
- Click **Clone** to clone the rule.
- Click **Cancel** to cancel the operation.

## Edit Network Rule

When you edit the network rule, follow these guidelines:

- You can only edit the custom rules.
- The rule name cannot be edited if the custom rule is assigned to a policy.
- If the custom rule assigned to a policy is edited, then you must republish the policy for the changes to take effect in the service.

### To edit a Network Rule


1. Go to  (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Click the **Network Rule** tab.
5. Select the network rule to edit.
6. Click **Edit Rule** to edit the network rule.

## Delete Network Rule

When you delete the network rule, follow these guidelines:

- You can delete only the custom network rules.
- You cannot delete the network rule if it is associated to a policy. You should first disassociate the network rule from the policy and then delete it.

### To delete a Network Rule


1. Go to  (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.

4. Click **Network Rule** tab.
5. Select a network rule to delete.
6. Click **Delete** to permanently delete the selected network rule.

## View Network Rule Details

This topic describes the steps to view the network rule details.


### To view Network Rule details

1. Go to  (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Click the **Network Rule** tab.
5. The list of network rules is displayed.
6. Click a row to view details about the selected network rule in the right panel.  
The various details of the network rule are displayed.



## Create an ESA Rule

This topic describes the steps to create an ESA rule.

### To create an ESA Rule

1. Go to  (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.  
The available rules are displayed.
4. Click **Event Stream Analysis Rule**.
5. In the ESA rule panel, click + **Create Rule** to add an ESA rule.

It navigates to **ESA Rules > Rules** view. For more information on creating new rules, see the section [Add a Rule Builder Rule](#).

**Note:** Analysts must have appropriate permissions to view the ESA rules under  (CONFIGURE) > **ESA Rules** and  (CONFIGURE) > **Policies** pages. For more information, see the **Source-server** section in the "Role Permissions" topic in the *System Security and User Management Guide*.

## Edit an ESA Rule


This topic provides instructions to edit an Event Stream Analysis (ESA) rule. When you edit a rule, ESA applies the updated criteria going forward. No changes are made to previously generated alerts.

For more information on editing an ESA rule, see [Edit, Duplicate or Delete a Rule](#).

## Delete an ESA Rule

You can delete one or more ESA rules. Once the ESA rule is deleted, the ESA rule will be removed from the available list.

### To delete an ESA Rule

1. Go to  (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.

The available rules are displayed.

4. Click **Event Stream Analysis Rule**.

The available ESA rules are displayed.

**Note:** Only Custom ESA rules that are not assigned to a policy will be available for deletion.

5. Select one or more custom ESA rules and click **Delete**.

A confirmation pop-up is displayed.

6. Click **Delete**.


## Filter Content Rules

The Filters panel allows you to filter the list of displayed contents under the content library based on the name, medium, date range, and source type.

This applies to the following content rule types:

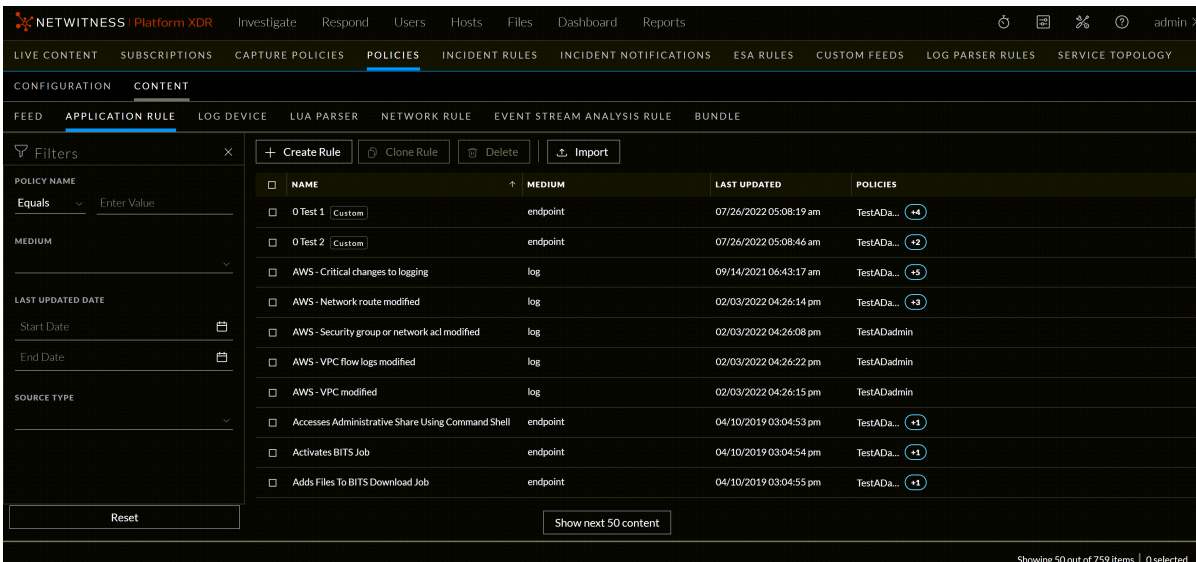
- Feed
- Application Rule
- Log Device
- Lua Parser
- Network Rule
- Event Steam Analysis Rule
- Bundle

### To filter the content rules

1. Go to  (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. Click **Content Library**.



- By default, the filters panel is hidden, click the  (Filters) icon in the toolbar to expand the filters panel.



The screenshot shows the NetWitness Platform XDR interface. The top navigation bar includes 'Platform XDR', 'Investigate', 'Respond', 'Users', 'Hosts', 'Files', 'Dashboard', and 'Reports'. Below this is a secondary navigation bar with 'LIVE CONTENT', 'SUBSCRIPTIONS', 'CAPTURE POLICIES', 'POLICIES', 'INCIDENT RULES', 'INCIDENT NOTIFICATIONS', 'ESA RULES', 'CUSTOM FEEDS', 'LOG PARSER RULES', and 'SERVICE TOPOLOGY'. The main content area is titled 'CONFIGURATION' and 'CONTENT', with sub-tabs for 'FEED', 'APPLICATION RULE', 'LOG DEVICE', 'LUA PARSER', 'NETWORK RULE', 'EVENT STREAM ANALYSIS RULE', and 'BUNDLE'. The 'APPLICATION RULE' tab is active, showing a 'Filters' panel on the left and a table of policies on the right.


The 'Filters' panel on the left has a search bar with 'Enter Value' and a dropdown menu set to 'Equals'. Below the search bar are sections for 'MEDIUM', 'LAST UPDATED DATE', and 'SOURCE TYPE', each with a dropdown menu and a 'Reset' button at the bottom.

The table of policies has the following columns: NAME, MEDIUM, LAST UPDATED, and POLICIES. The data rows are as follows:

NAME	MEDIUM	LAST UPDATED	POLICIES
0 Test 1 Custom	endpoint	07/26/2022 05:08:19 am	TestADa... +4
0 Test 2 Custom	endpoint	07/26/2022 05:08:46 am	TestADa... +2
AWS - Critical changes to logging	log	09/14/2021 06:43:17 am	TestADa... +5
AWS - Network route modified	log	02/03/2022 04:26:14 pm	TestADa... +3
AWS - Security group or network ad modified	log	02/03/2022 04:26:08 pm	TestADadmin
AWS - VPC flow logs modified	log	02/03/2022 04:26:22 pm	TestADadmin
AWS - VPC modified	log	02/03/2022 04:26:15 pm	TestADadmin
Accesses Administrative Share Using Command Shell	endpoint	04/10/2019 03:04:53 pm	TestADa... +1
Activates BITS Job	endpoint	04/10/2019 03:04:54 pm	TestADa... +1
Adds Files To BITS Download Job	endpoint	04/10/2019 03:04:55 pm	TestADa... +1

At the bottom of the table, there is a 'Show next 50 content' button. The status bar at the bottom right indicates 'Showing 50 out of 759 items | 0 selected'.

- To search by policy name:
  - Set the filter option to **Contains** operator from the drop-down list and start typing the name of the policy. Type one character and a list of policies that contain that character is displayed, as you continue to type the list is filtered to match.
  - Set the filter option to **Equals** operator from the drop-down list and enter the full name. The particular content type will be displayed.
- To filter by medium, select one or more mediums from the **Medium** drop-down list. The options are listed below:
  - endpoint**
  - log**
  - log and packet**
  - packet**
- To filter by date range, under the **Last Update date**, select the start date and end date from the date fields.
 

For example, to filter policies that were updated between July 1 and July 30, you select July 1 as the start date and July 30 as the end date. You must enter dates in **mm/dd/yyyy** format or you click and pick dates from a calendar.
- To filter by source type, select one or more sources from the **Source Type** drop-down list. The options are listed below:
  - Custom**
  - Live**
- To hide, click the  icon at the top-right of the panel.

The contents are displayed in the right panel according to the filter you selected. Click **Reset** to clear the existing filter results.

## Manage Groups


This section contains:

- [Create a Group](#)
- [View a Group](#)
- [Delete a Group](#)
- [Edit a Group](#)
- [Filter Groups](#)

### Create a Group

You can create a group with one or more services and assign one policy to it. Groups may be created without any assigned policy; however, a policy must be assigned to a group and Published in order for any content changes to take effect.

#### To create a Group

1. Go to  (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Groups**.
4. In the tool bar, click + **Create New**.
5. In the **New Group** panel, do the following:
  - Enter the name of the group.
  - Enter the description for the group.
6. Click **Next**.
7. In the **Define Group**, click + to assign services to the group.

**Note:**

- A service is disabled if it is assigned to another group.
- A service is disabled if it is not managed by Policy-based Centralized Content Management.
- ESA Services are not disabled when assigned to a group, as the ESA services can be assigned to more than one group.

8. Click **Next**.
9. In the **Assign Policies**, click + to assign policies to a group. You can assign only one policy to any particular group.


10. Do any one of the following:


- Click **Save and Publish** to save and publish the settings.
  - To publish all the content, click **Publish All**.
  - To publish only the content that is not published on the service, click **Publish Changes**.
  - To cancel the publish content dialog, click **Cancel**.
- Click **Save and Close** to save the settings.

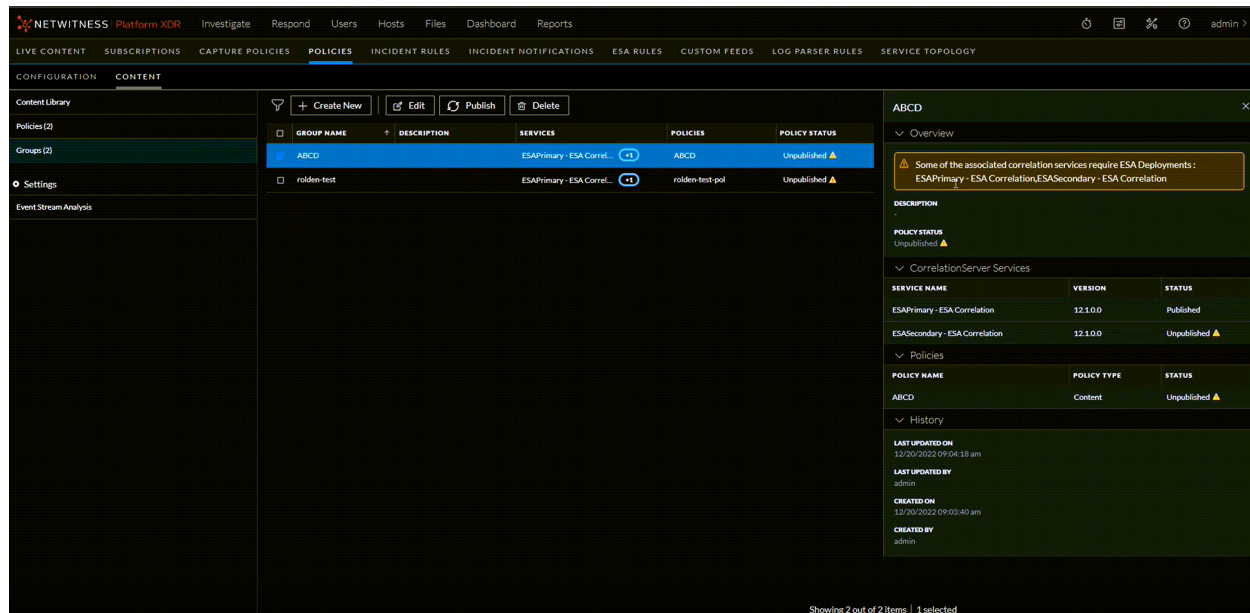
## View a Group

This topic describes the steps to view the properties of Group.

### To view the properties of the selected Group




1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.
3. Click **Groups**. The available groups are displayed.
4. Click a row to view details about the selected group in the right panel.


**Caution:** An icon  is displayed in the Groups View indicating policy status unpublished, if any services are part of the selected group and do not have any deployment then some of the associated correlation services require ESA deployments.



The screenshot shows the NetWitness Platform XDR interface. The top navigation bar includes 'NETWISNESS Platform XDR' and various menu items like 'Investigate', 'Respond', 'Users', 'Hosts', 'Files', 'Dashboard', and 'Reports'. The main interface is divided into several sections:

- Content Library:** Shows 'Policies (2)' and 'Groups (2)'. The 'Groups (2)' section is expanded to show a table of groups.
- Policies Table:**

GROUP NAME	DESCRIPTION	SERVICES	POLICIES	POLICY STATUS
ABCD		ESAPrimary - ESA Correl...	ABCD	Unpublished 
rolden-test		ESAPrimary - ESA Correl...	rolden-test pol	Unpublished 
- Right Panel (ABCD):**
  - Overview:** Shows a warning: 'Some of the associated correlation services require ESA Deployments: ESAPrimary - ESA Correlation, ESASSecondary - ESA Correlation'.
  - DESCRIPTION:** Shows 'POLICY STATUS: Unpublished | SERVICE NAME | VERSION | STATUS |
| --- | --- | --- |
| ESAPrimary - ESA Correlation | 12.1.0.0 | Published |
| ESASSecondary - ESA Correlation | 12.1.0.0 | Unpublished |
  - Policies:**


POLICY NAME	POLICY TYPE	STATUS
ABCD	Content	Unpublished 
  - History:**
    - LAST UPDATED ON:** 12/20/2022 09:04:18 am
    - LAST UPDATED BY:** admin
    - CREATED ON:** 12/20/2022 09:03:40 am
    - CREATED BY:** admin

At the bottom right, it says 'Showing 2 out of 2 items | 1 selected'.

## Delete a Group

You can delete one or more groups. Once the group is deleted, all services will be removed from the group and all the policy content will be deleted from the services.

## To delete a Group

1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.
3. Click **Groups**. The available groups are displayed.
4. Select one or more Groups and click **Delete**.  
The Delete Groups dialog is displayed.
5. To delete the deployed content from the services upon deleting the group, select the option **Delete deployed content from the services on group removal**. For ESA service, the content will be deleted upon deleting the group.
6. Click **Delete** to permanently delete the selected group.  
The confirmation message is displayed.


### Note:

- For a group with multiple services, even if we fail to delete a particular service under the group, the other services will get deleted. The service which is not deleted will be in **Failed** state.
- The group status changes to **Failed** if group deletion fails for any particular reason.

## Edit a Group

You can edit the properties of the group at any point in time. The status of the updated group is unpublished if you change the service or policies in a group. If you just change the group name and description, then the status remains published (if it is already published).

## To edit the selected Group

1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.
3. In the left panel, click **Group**. The available groups are displayed.
4. Select a group to edit and click **Edit**.
5. Make the required changes in the group.
6. Do any one of the following:
  - Click **Save and Publish** to save and publish the policy.

### Note:

- While removing a service from the group, you can opt to either delete the content of the service and remove the service or just remove the service from the group.
- While removing the group from the policy, the ESA content will be deleted by default.

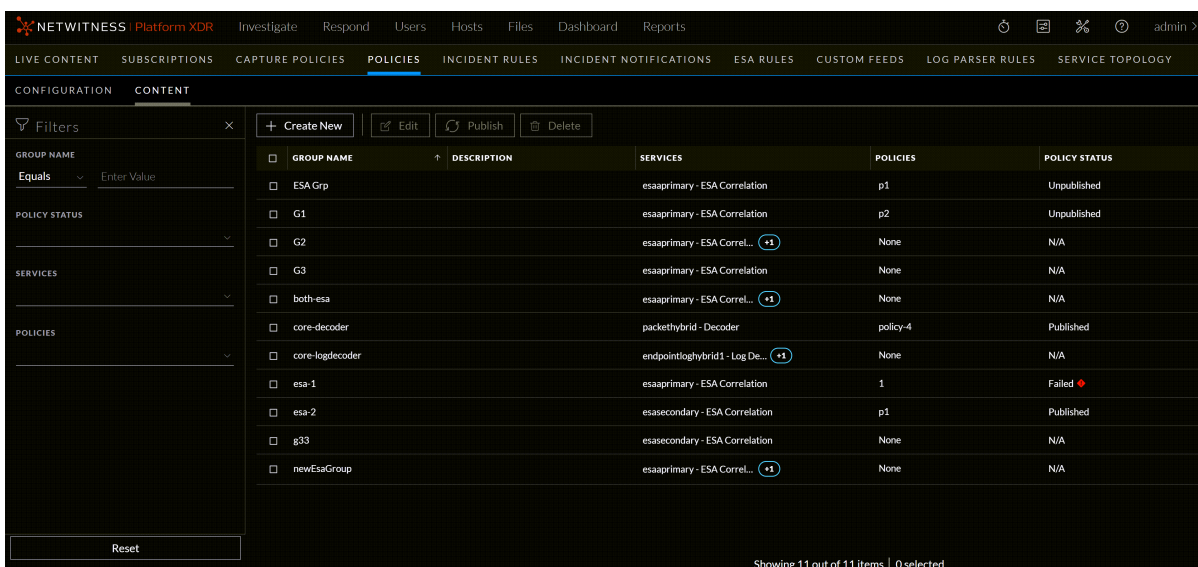
- The policy will be listed under the Unpublished category.
- Click **Save and Close** to save the settings and return to the Policies view.

## Filter Groups

The Filters panel allows you to filter the list of displayed groups based on the group name, policy status, services, and policies.


### To filter the groups

1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.
3. Click **Groups**.
4. By default, the filters panel is hidden, click the  (Filters) icon in the toolbar to expand the filters panel.



GROUP NAME	DESCRIPTION	SERVICES	POLICIES	POLICY STATUS
<input type="checkbox"/> ESA Grp	esaprimary - ESA Correlation		p1	Unpublished
<input type="checkbox"/> G1	esaprimary - ESA Correlation		p2	Unpublished
<input type="checkbox"/> G2	esaprimary - ESA Correl... <sup>+1</sup>		None	N/A
<input type="checkbox"/> G3	esaprimary - ESA Correlation		None	N/A
<input type="checkbox"/> both-esa	esaprimary - ESA Correl... <sup>+1</sup>		None	N/A
<input type="checkbox"/> core-decoder	packethybrid - Decoder		policy-4	Published
<input type="checkbox"/> core-logdecoder	endpointloghybrid1 - Log De... <sup>+1</sup>		None	N/A
<input type="checkbox"/> esa-1	esaprimary - ESA Correlation		1	Failed <span style="color: red;">❗</span>
<input type="checkbox"/> esa-2	esasecondary - ESA Correlation		p1	Published
<input type="checkbox"/> g33	esasecondary - ESA Correlation		None	N/A
<input type="checkbox"/> newEsaGroup	esaprimary - ESA Correl... <sup>+1</sup>		None	N/A

5. To search by group name:
  - Set the filter option to **Contains** operator from the drop-down list and start typing the name of the group. Type one character and a list of groups that contain that character is displayed, as you continue to type the list is filtered to match.
  - Set the filter option to **Equals** operator from the drop-down list and enter the full name. The particular group will be displayed.
6. To filter by policy status, select one or more statuses from the **Policy Status** drop-down list. The options are listed below:
  - **Published:** Policies that are published to use.
  - **Unpublished:** Policies that are saved but not published.
  - **Failed:** Policies that are failed to publish.
  - **N/A:** Policies for which publication status is not applicable.
7. To filter by services, select one or more services from the **Services** drop-down list. For example, Log Decoder.

8. To filter by policies, select one or more policies from the **Policies** drop-down list. You can also search for the name of the policies from this list.
9. To hide, click the  icon at the top-right of the panel.  
The groups are displayed in the right panel according to the filter you selected. Click **Reset** to clear the existing filter results.

## Manage Policies

Policies contain content and subscription settings used to assign and manage content within a Group.

**IMPORTANT:** The customers should note that, while publishing the first policy to a service, all previous content except custom feeds, will be deleted. Ensure that all custom content are migrated to Content Library before publishing the first policy.


This section contains:

- [Create and Publish Policies](#)
- [Clone a Policy](#)
- [Delete a Policy](#)
- [Edit a Policy](#)
- [View a Policy](#)
- [Enable Content for a Policy](#)
- [Disable Content for a Policy](#)
- [Subscribe Content for a Policy](#)
- [Unsubscribe Content for a Policy](#)
- [Filter Policies](#)
- [Filter Policy Content Details](#)
- [Merge Policy with ESA Content](#)

## Create and Publish Policies

You can create a policy and assign it to one or more groups.

### To create a Policy

1. Go to  (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. Click **Policies**.  
The available policies are displayed.
4. Click + **Create New** to add a new policy.

5. In the **New Policy** panel, do the following:
  - Enter a unique policy name.
  - Enter a description for the policy.
6. Click **Next**.
7. In the **Available Content**, select the content type and click + to add the content to the policy. After you add the content, you can enable subscription (if required) by clicking subscribed toggle. Once the content is subscribed the updates are pushed automatically.

**Note:** Subscription is not allowed for custom content.

The screenshot displays the 'Create Content Policy' interface in the NETWITNESS Platform XDR. The 'Define Policy' section is active, showing a list of available content and a list of selected content. The 'Available Content' table has the following data:

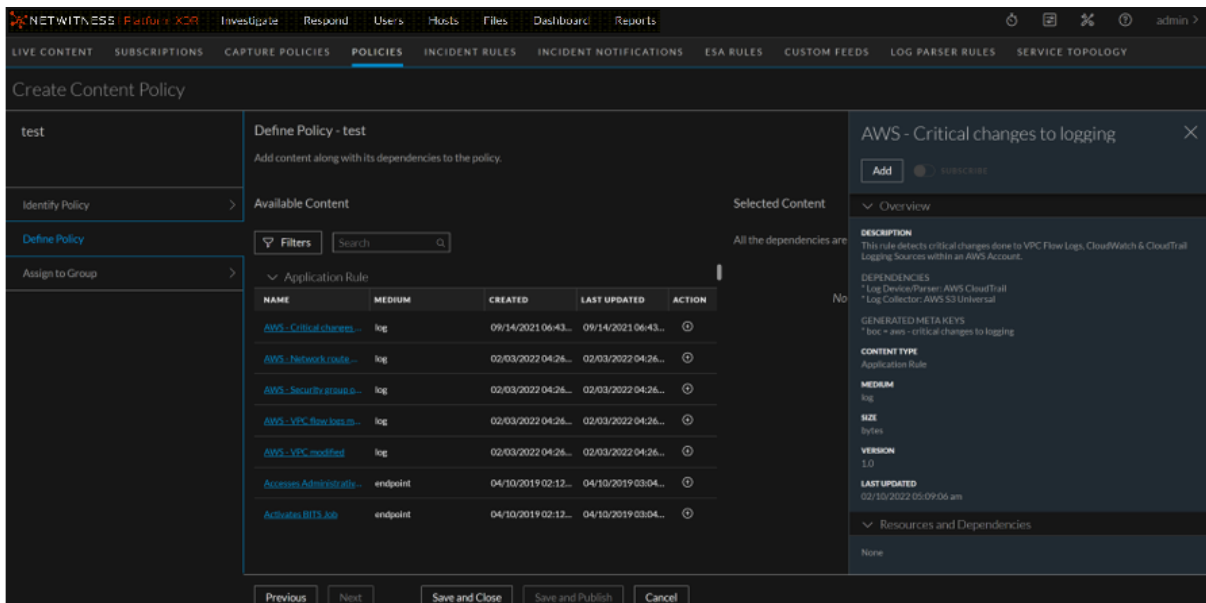
NAME	MEDIUM	CREATED	LAST UPDATED	ACTION
aws_vpc_flow_logs	log	02/03/2022 04:2...	02/03/2022 04:2...	⊕
aws_vpc_flow_logs	log	02/03/2022 04:2...	02/03/2022 04:2...	⊕
Accesses Administrative	endpoint	04/10/2019 02:1...	04/10/2019 03:0...	⊕
Activates BITS Job	endpoint	04/10/2019 02:1...	04/10/2019 03:0...	⊕
Add Files To BITS Da	endpoint	04/10/2019 02:1...	04/10/2019 03:0...	⊕
Add Firewall Rule	endpoint	04/10/2019 02:1...	04/10/2019 03:0...	⊕


The 'Selected Content' table has the following data:

NAME	MEDIUM	CREATED	LAST UPDATED	SUBSCRIBED	⊕ ALL
aws_CriticalChanges	log	09/14/2021...	09/14/2021...	<input checked="" type="checkbox"/>	⊕
aws_NetworkRoute	log	02/03/2022...	02/03/2022...	<input type="checkbox"/>	⊕
aws_SecurityGroup	log	02/03/2022...	02/03/2022...	<input type="checkbox"/>	⊕

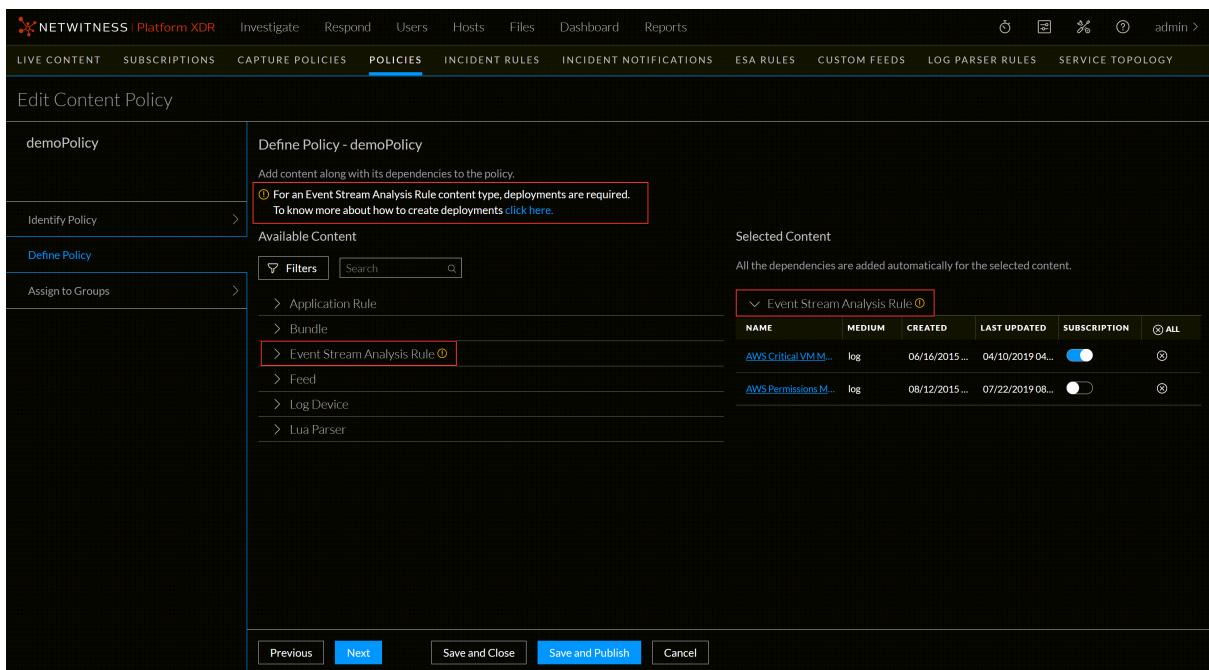
**Note:**

- All the dependencies are added automatically for the selected content. You can click on the content name highlighted in blue and look for details such as content description, content type, resources and dependencies and so on. You can also add and subscribe the resource from the details view.



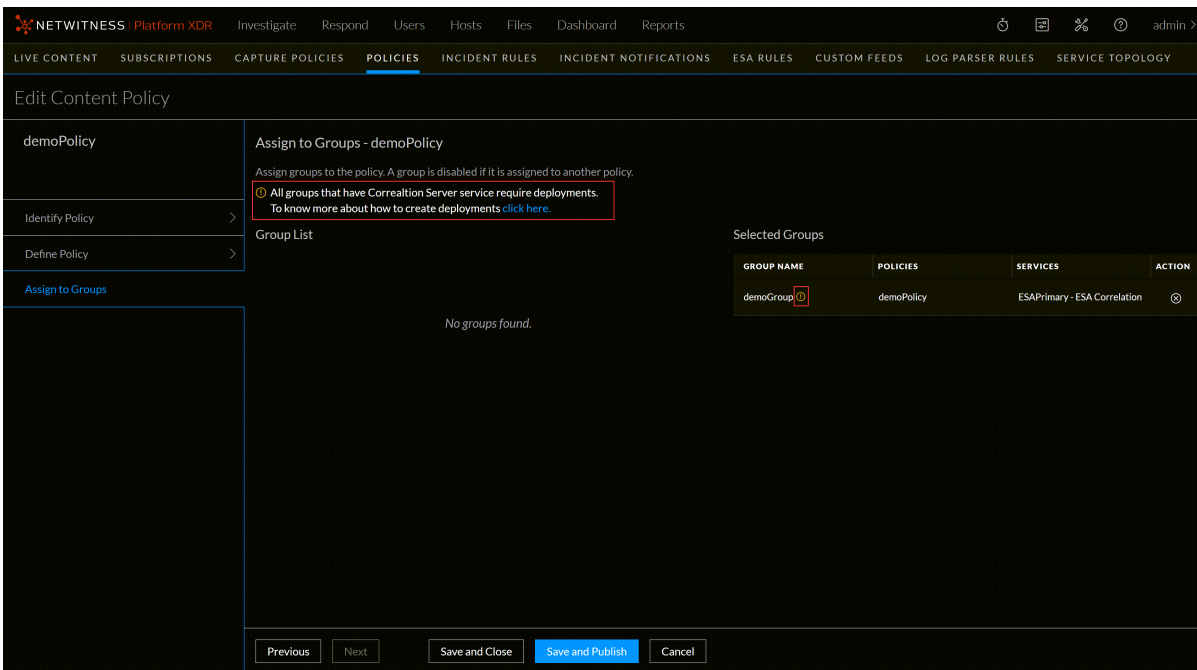
A caution icon  is displayed to create a deployment on three scenarios.

- To implement the **Event Stream Analysis Rule** content type, you must have a deployment.

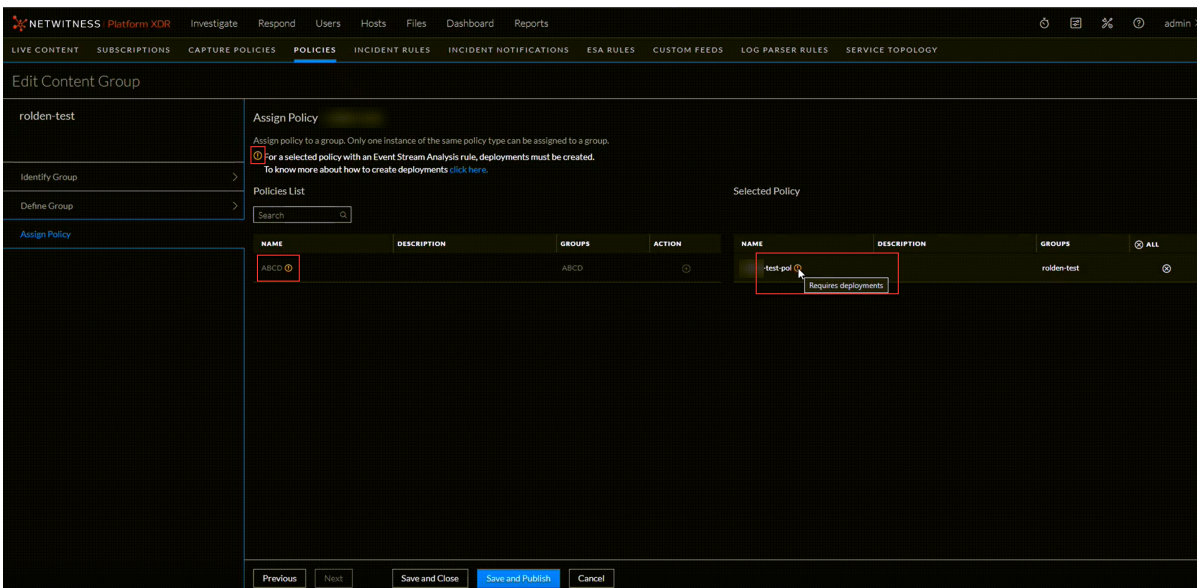


- All groups that have correlation server service must have a deployment.





- For any selected policy with an ESA rule, deployment are must be created.



To create and manage deployments, refer to [Manage Deployments](#) feature.

8. In the Group List, click + to assign groups to the policy.

**Note:** A group is disabled if another policy of the same type is already assigned to this group.

9. Click **Save and Publish** to save and publish the settings.

**IMPORTANT:** Once the publish is successful, you can view only the published content on the service while publishing the policy for the first time.

**Note:**

- While publishing the first policy to a service, all previous content except custom feeds, will be deleted. Ensure that all custom content are migrated to content library before publishing the first policy.
- You can also publish a policy from **Policy Details** screen. For more information on publishing a policy from **Policy Details** screen, refer [View a Policy](#) feature.

10. Click **Cancel** to cancel the publish content dialog.
11. Click **Save and Close** to save the settings.


**IMPORTANT:**

When first applying a Content Policy to manage content, the existing Live and custom content on the service (excluding Custom Feeds) will be removed and replaced with the Policy content. You should compare the existing service content with the policy before applying to ensure required content is added to the policy. Endpoint risk scoring requires certain application rules. Refer [Endpoint Risk Scoring Rules](#) to view the list of these application rules.

## Clone a Policy

When you clone a policy, all the content from the old policy is copied to the new policy. The cloned policy can be assigned to a new group. You can clone only one policy at a time.


### To clone a Policy

1. Go to  (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. Click **Policies**. The available policies are displayed.
4. Select a policy to clone and in the More actions drop-down list in the tool bar, click **Clone**.  
The policy is cloned successfully.

## Delete a Policy

Deleting a policy removes all content from the associated group.

### To delete a Policy

1. Go to  (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. Click **Policies**. The available policies are displayed.
4. Select one or more policies and in the More actions drop-down list in the tool bar, click **Delete**.  
The **Delete Policies** dialog is displayed.
5. To delete the deployed content from the group's services upon deleting the policy, select the option **Delete deployed content from the group's services on policy removal**. For ESA service, the content will be deleted upon deleting the policy.
6. Click **Delete** to permanently delete the selected policy.

Deletion will take immediate effect and the policy will no longer be available in any group.


**Note:**

- The services associated with this policy still require a restart if the restart is pending.
- You can also delete a policy from **Policy Details** screen. For more information on deleting a policy from **Policy Details** screen, refer [View a Policy](#) feature.
- The policy status changes to **Failed** if policy deletion fails for any particular reason.

## Edit a Policy

You can edit the content and settings of the policies. Once the policy is edited, the changes in the policy are reflected upon saving the policy. The changes are applied to the service once published. After saving and before publishing, the publication status of the changed policy is set to **Unpublished** if any settings are changed.

### To edit a Policy

1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.
3. Click **Policies**. The available policies are displayed.
4. Select a policy to edit and click **Edit**.
5. Make the required changes in policy.
6. Do any one of the following:
  - Click **Save and Publish** to save and publish the policy. The policy will be listed under the Unpublished category.

**Note:**

- While removing a group from the policy, you can either delete the content of the service and remove the group or just remove the group from the policy.
- While removing the group from the policy, the ESA content will be deleted by default.

- Click **Save and Close** to save the settings and return to the Policies view.

**Note:** You can also edit a policy from **Policy Details** screen. For more information on editing a policy from **Policy Details** screen, see [View a Policy](#) feature.


## View a Policy

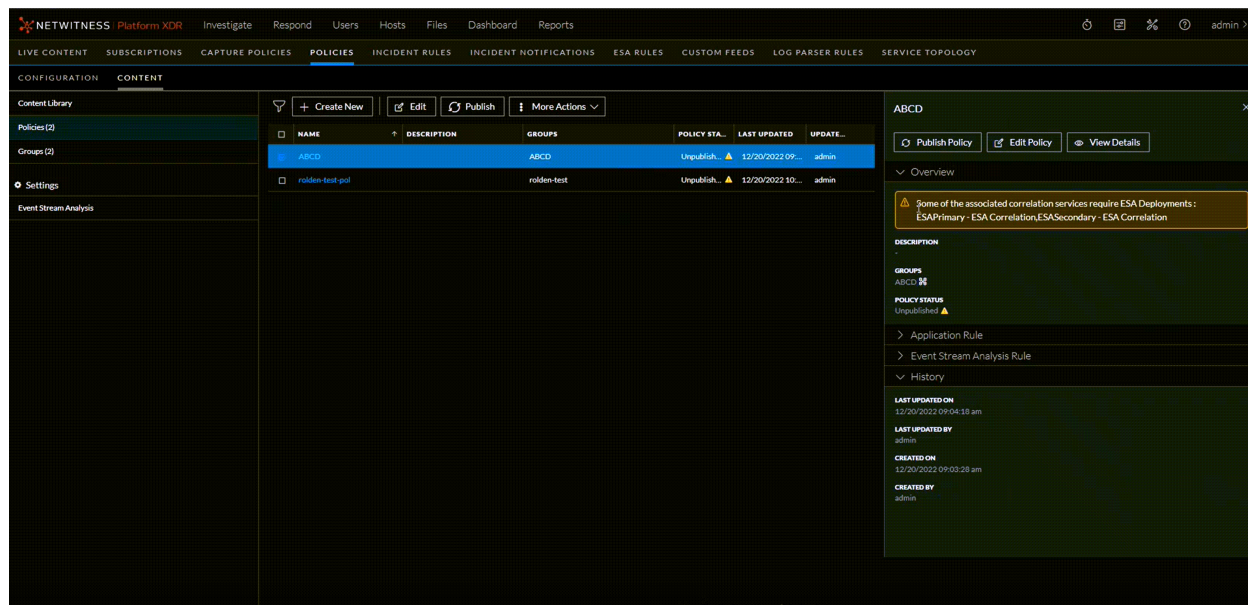
This topic describes the steps to view the properties of a Policy.

### To view properties of the selected Policy

1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.

3. Click **Policies**. The available policies are displayed.

**Caution:** An icon  is displayed in the Policy View indicating policy status unpublished, if any services are part of the selected policy and do not have any deployment then some of the associated correlation services require ESA deployments.







4. From the policy listing page, you can perform the following actions:

- Select a policy and click **Edit** to edit the policy. For more information on editing a policy, see [Edit a Policy](#) feature.
- Select the policy and click **Publish** to publish the policy if the policy is unpublished.
- Select the policy and click **More Actions** > **Assign to Groups** to assign policy to available group.
- Select the policy and click **More Actions** > **Clone** to clone the policy. For more information on cloning a policy, see [Edit a Policy Clone a Policy](#) feature.
- Select the policy and click **More Actions** > **Delete** to delete the policy. For more information on deleting a policy, see [Delete a Policy](#) feature.
- Select the policy and click **More Actions** > **Force Publish** to force publish the policy. This action allows you republish all the content irrespective of the policy status.

5. Click a row to view details about the selected policy.

6. To change the order of application rule assigned to the policy, do the following:

1. To move the application rule or network down the order, click  in the **Order** column.
2. To move the application rule up the order, click  in the **Order** column.
3. You can also manually enter the order number in the **Order** column.

7. To change the order of network rule assigned to the policy, do the following:
  1. Click **Network Rules** tab.
  2. To move the network rule or network down the order, click  in the **Order** column.
  3. To move the network rule up the order, click  in the **Order** column.
  4. You can also manually enter the order number in the **Order** column.

**IMPORTANT:** It is recommended not to order application rules or network rules deployed on the service from Service Config page if the service is part of Centralized Content Management.

8. From the policy details page, you can perform the following actions:
  - To edit the policy, click **Edit Policy**. For more information on editing a policy, see [Edit a Policy](#) feature.
  - To delete the policy, click **Delete Policy**. For more information on deleting a policy, see [Delete a Policy](#) feature.
  - To publish the policy, click **Publish Policy**. For more information on creating and publishing a policy, see [Create and Publish Policies](#) feature.
  - To force publish a policy, click **Force Publish**. This action allows you republish all the content irrespective of the policy status.
  - To enable or disable subscription, click **Subscribe** or **Unsubscribe** respectively.


**Note:**

- Subscription is not allowed for custom content.
- The **Subscribe** and **Unsubscribe** button is disabled if any one of the content selected is custom.

## Enable Content for a Policy

This topic describes the steps to enable the content for a Policy.


### To enable content

1. Go to  (**CONFIGURE**) > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Policies**.
4. Click the policy name to view the policy details.
5. In the **Application Rule**, **Network Rule**, **Feed**, **Log Device** or **LUA Parser** panel, click the row to select the content to be enabled. You can either select all content or select any specific content to be enabled.
6. Click **Enable**.

## Disable Content for a Policy

This topic describes the steps to disable the content for a Policy.

## To disable content

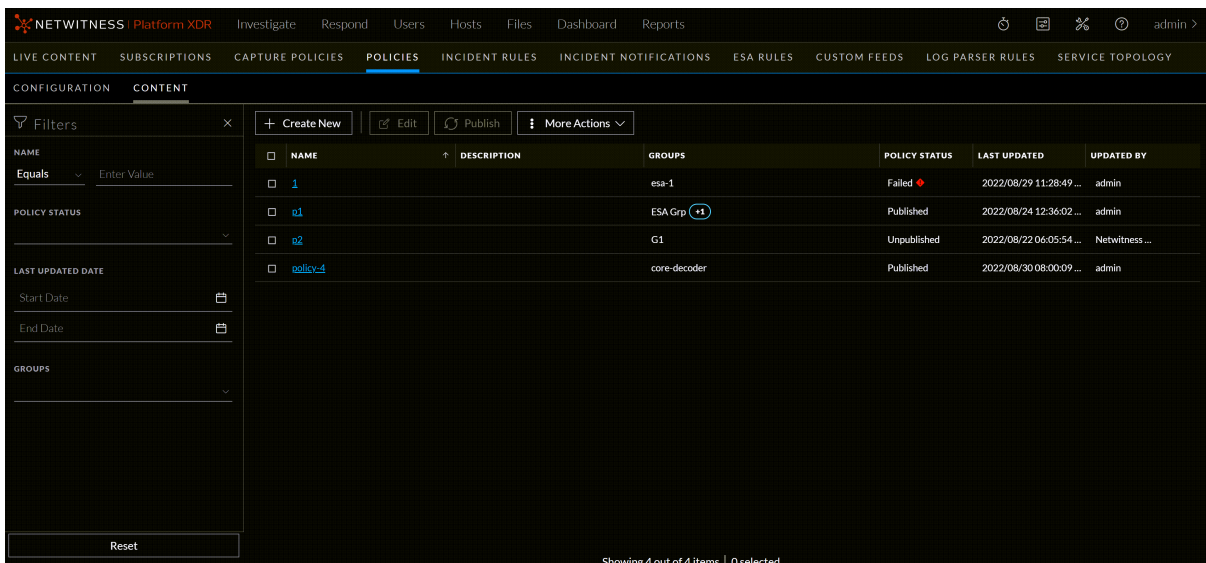
1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.
3. In the left panel, click **Policies**.
4. Click the policy name to view the policy details.
5. In the **Application Rule**, **Network Rule**, **Feed**, **Log Device** or **LUA Parser** panel, click the row to select the content to be disabled. You can either select all content or select any specific content to be disabled.
6. Click **Disable**.

## Filter Policies

The Filters panel allows you to filter the list of displayed policies based on the name, policy status, date range, and groups.

### To filter the policies

1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.
3. Click **Policies**.
4. By default, the filters panel is hidden, click the  (Filters) icon in the toolbar to expand the filters panel.




The screenshot shows the NetWitness Platform XDR interface. The top navigation bar includes 'NETWISNESS | Platform XDR' and various menu items like 'Investigate', 'Respond', 'Users', 'Hosts', 'Files', 'Dashboard', and 'Reports'. Below this is a secondary navigation bar with 'LIVE CONTENT', 'SUBSCRIPTIONS', 'CAPTURE POLICIES', 'POLICIES', 'INCIDENT RULES', 'INCIDENT NOTIFICATIONS', 'ESA RULES', 'CUSTOM FEEDS', 'LOG PARSER RULES', and 'SERVICE TOPOLOGY'. The main content area is titled 'CONFIGURATION' and 'CONTENT'. On the left, a 'Filters' panel is expanded, showing options for 'NAME' (set to 'Equals'), 'POLICY STATUS', 'LAST UPDATED DATE' (with 'Start Date' and 'End Date' fields), and 'GROUPS'. The main table displays a list of policies with columns for 'NAME', 'DESCRIPTION', 'GROUPS', 'POLICY STATUS', 'LAST UPDATED', and 'UPDATED BY'. The table contains four rows of data, with the second row highlighted. At the bottom right of the table, it says 'Showing 4 out of 4 items | 0 selected'.

NAME	DESCRIPTION	GROUPS	POLICY STATUS	LAST UPDATED	UPDATED BY
1		esa-1	Failed	2022/08/29 11:28:49 ...	admin
a1		ESA Grp	Published	2022/08/24 12:36:02 ...	admin
a2		G1	Unpublished	2022/08/22 06:05:54 ...	Netwitness ...
policy-4		core-decoder	Published	2022/08/30 08:00:09 ...	admin

5. To search by name:
  - Set the filter option to **Contains** operator from the drop-down list and start typing the name of the policy. Type one character and a list of policies that contain that character is displayed, as you continue to type the list is filtered to match.

- Set the filter option to **Equals** operator from the drop-down list and enter the full name. The particular policy will be displayed.
6. To filter by policy status, select one or more statuses from the **Policy Status** drop-down list. The options are listed below:
    - **Published**: Policies that are published to use.
    - **Unpublished**: Policies that are saved but not published.
    - **Failed**: Policies that are failed to publish.
    - **N/A**: Policies for which publication status is not applicable.
  7. To filter by date range, under the **Last Update date**, select the start date and end date from the date fields.

For example, to filter contents that were updated between July 1 and July 30, you select July 1 as the start date and July 30 as the end date. You must enter dates in **mm/dd/yyyy** format or you click and pick dates from a calendar.
  8. To filter by groups, select one or more groups from the **Groups** drop-down list. You can also search for the name of the groups from this list.
  9. To hide, click the  icon at the top-right of the panel.

The groups are displayed in the right panel according to the filter you selected. Click **Reset** to clear the existing filter results.


## Filter Policy Content Details

The Filters panel allows you to filter the list of displayed content in the policy details view based on the name, medium, source type, enabled/disabled status, subscription status, a resource created date, and last updated date.

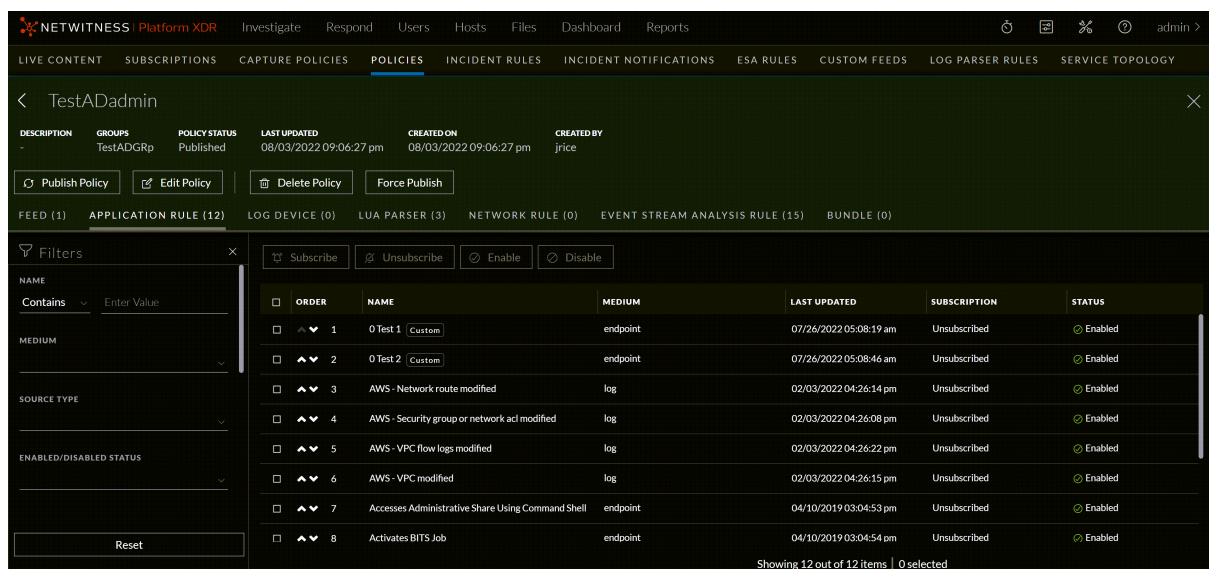
This applies to the following content types:


- Feed
- Application Rule
- Log Device
- Lua Parser
- Network Rule
- Event Steam Analysis Rule
- Bundle

## To filter policy content details

1. Go to  (**CONFIGURE**) > **Policies**.
2. In the policies panel, click **Content**.
3. Click **Policies**. The available policies are displayed.
4. Do one of the following:
  - Click a policy name.
  - Click a row to view details about the selected policy and click **View Details**.

The policy details view is displayed.



5. By default, the filters panel is hidden, click the  (Filters) icon in the toolbar to expand the filters panel.
6. To search by name:
  - Set the filter option to **Contains** operator from the drop-down list and start typing the name of the content rules. Type one character and a list of content rules that contain that character is displayed, as you continue to type the list is filtered to match.
  - Set the filter option to **Equals** operator from the drop-down list and enter the full name. The particular content type will be displayed.
7. To filter by medium, select one or more mediums from the **Medium** drop-down list. The options are listed below:
  - **endpoint**
  - **log**
  - **log and packet**
  - **packet**




8. To filter by source type, select one or more sources from the **Source Type** drop-down list. The options are listed below:
  - **Custom**
  - **Live**
9. To filter by enabled/disabled status, select one or more statuses from the **Enabled/Disabled Status** drop-down list. The options are listed below:
  - **Enabled**
  - **Disabled**

**Note:** Enabled/Disabled Status filtering is not applicable to Event Stream Analysis Rule content.


10. To filter by subscription status, select one or more statuses from the **Subscription** drop-down list. The options are listed below:
  - **Subscribed**
  - **Unsubscribed**
11. To filter by a resource created date range, under the **Resource Created Date**, select the start date and end date from the date fields.

For example, to filter contents that were created between July 1 and July 30, you select July 1 as the start date and July 30 as the end date. You must enter dates in **mm/dd/yyyy** format or you click and pick dates from a calendar.
12. To filter by date range, under the **Last Update date**, select the start date and end date from the date fields.

For example, to filter contents that were updated between July 1 and July 30, you select July 1 as the start date and July 30 as the end date. You must enter dates in **mm/dd/yyyy** format or you click and pick dates from a calendar.
13. To hide, click the  icon at the top-right of the panel.


The contents are displayed in the right panel according to the filter you selected. Click **Reset** to clear the existing filter results.

## Merge Policy with ESA Content

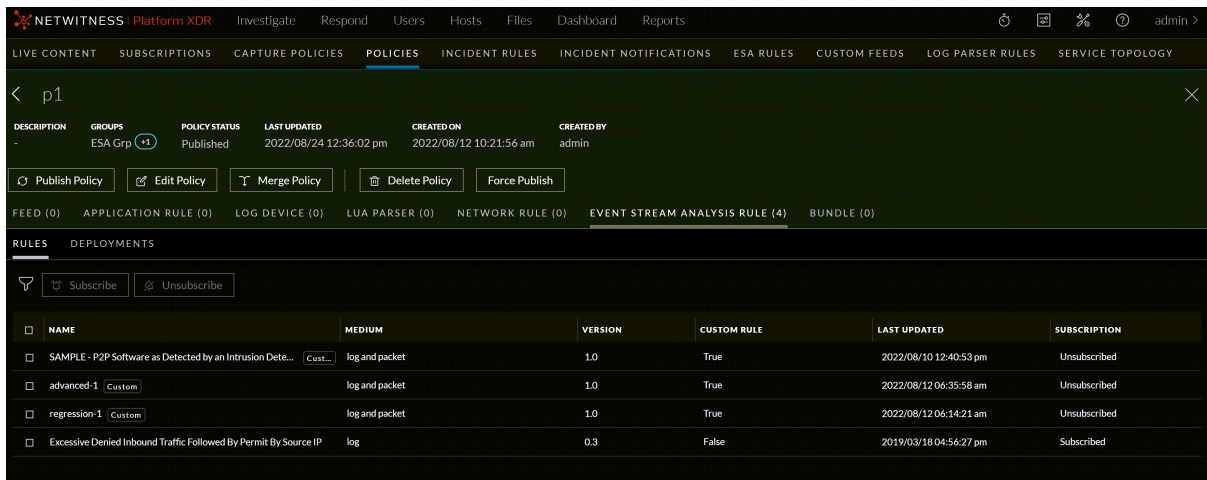
From the 12.1 version, the ESA content is managed through the  (**CONFIGURE**) > **Policies** page. After you upgrade to the 12.1 version, all the existing ESA deployments will be migrated to the policies and groups view. The **Merge Policy** button will be available only for the policy having ESA content and can only be merged with a policy with no ESA content.

**Note:** On merging a policy with another policy, the original policy gets deleted, and the other policy gets updated with the original policy content.

### To merge Policy with an ESA Content

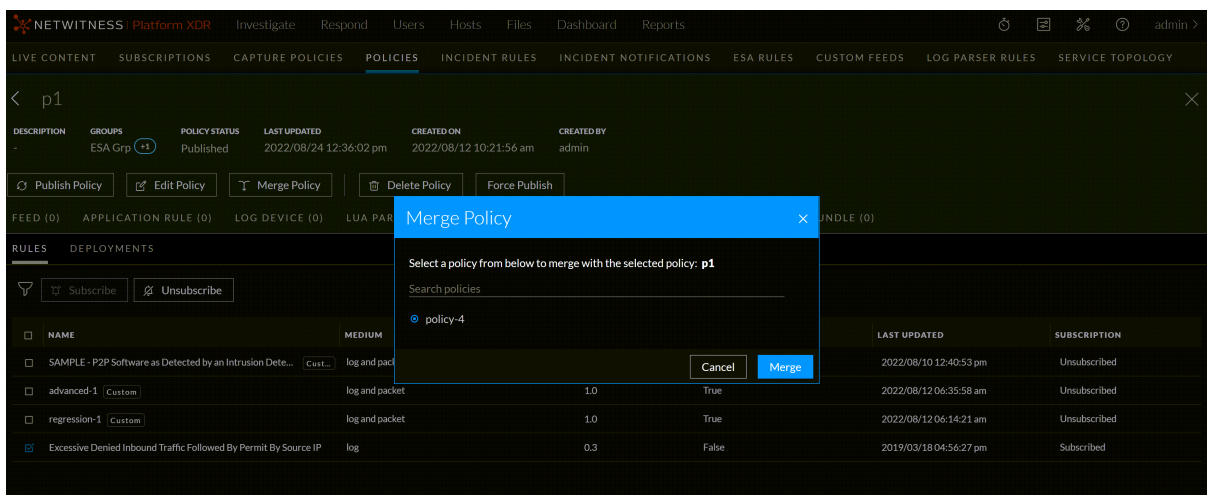
1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.
3. Select a policy having ESA content to merge with another policy.

The selected policy with ESA content view is displayed.



4. Click **Merge Policy**.

The Merge Policy dialog is displayed.



5. Select a policy from the list or search for the name and Click **Merge**.  
A confirmation pop-up is displayed.
6. Click **Confirm**.

### Manage ESA Datasources


This section contains:

- [View an ESA Datasource](#)
- [Add an ESA Datasource](#)
- [Edit an ESA Datasource](#)
- [Delete an ESA Datasource](#)

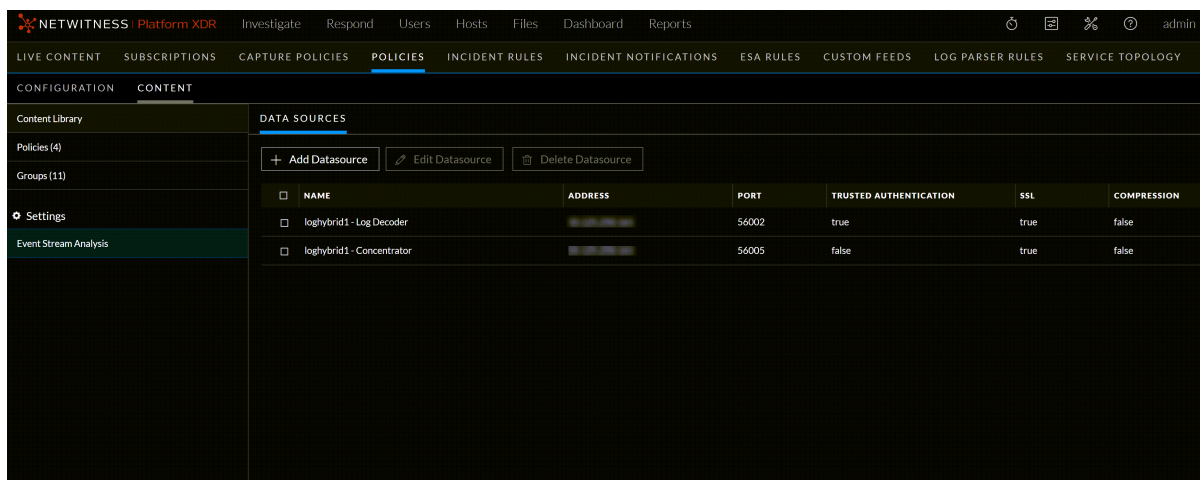
## View an ESA Datasource

This topic describes the steps to view the ESA datasources available.

### To view an ESA Datasource

1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.
3. Under **Settings**, click **Event Stream Analysis** > **Data Sources**.


The available datasources are displayed.



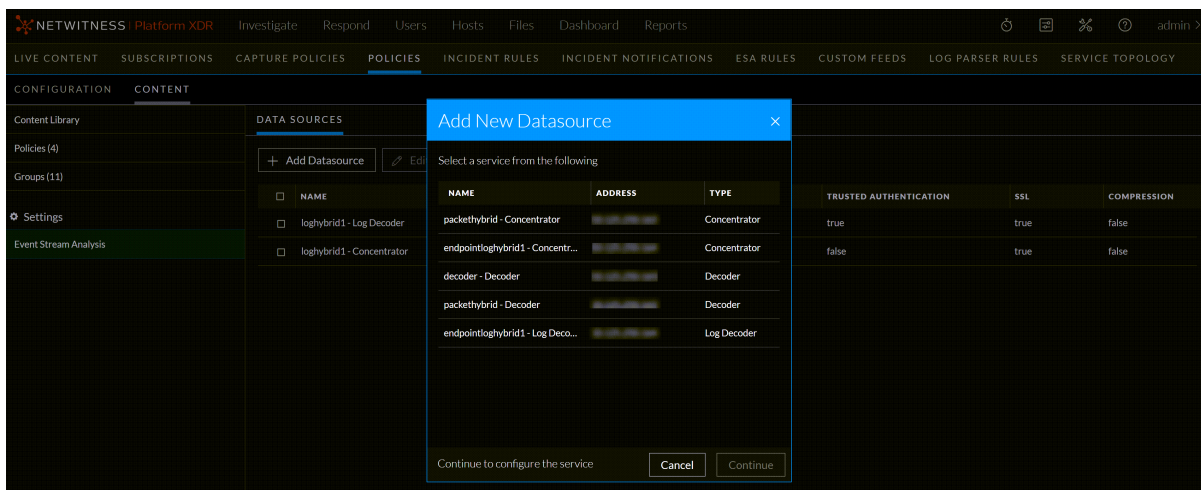
## Add an ESA Datasource

You can add one or more ESA data sources, such as Concentrators, to use for your selected ESA Service. This enables you to specify different data sources for each deployment.

### To add an ESA Datasource

1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.
3. Under **Settings**, click **Event Stream Analysis** > **Data Sources**.
4. Click **+ Add Datasource**.

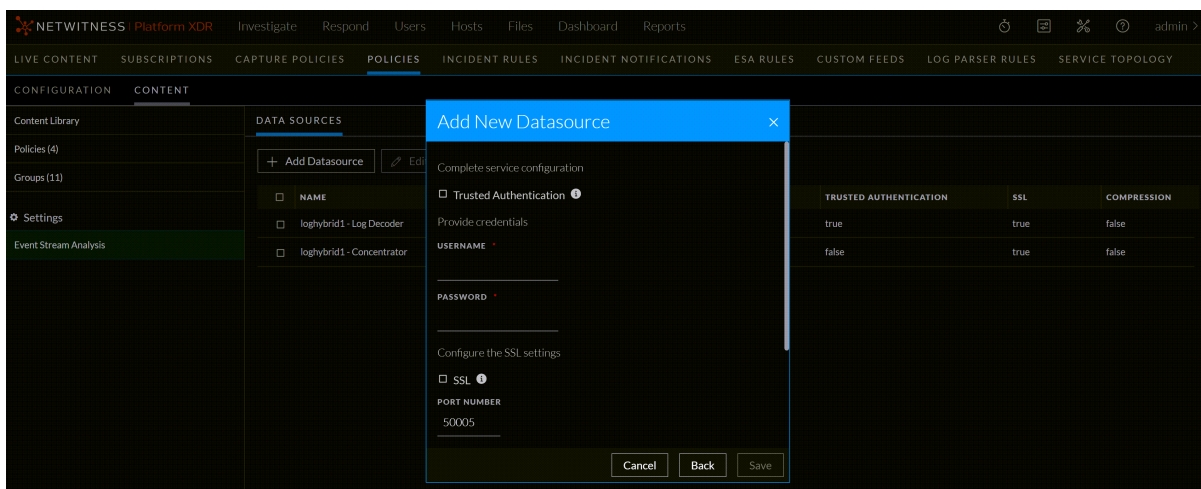
The Add New Datasource dialog is displayed.



**Note:** You can add a Log Decoder as a data source for ESA. But, it is better to add a Concentrator to take advantage of undivided aggregation as the Decoder may have other processes aggregating from it.

5. Select a service and click **Continue**.

**Note:** You can add only one service at a time.



6. Do one of the following:
  - Select the **Trusted Authentication** checkbox.
  - Enter your credentials (username and password) for the datasource.

**Note:**

- If you select **Trusted Authentication** instead of username and password. This option will enable the use of SSL by default. However, you can still configure the compression settings.
- If you choose to enter your username and password. You can configure both SSL and compression settings.

7. To enable the SSL settings, select the **SSL** checkbox. You can set your desired port number.

**IMPORTANT:** Ensure that you turn on SSL only if necessary, in order to avoid performance impact on the SSL protocol.

8. (Optional) You have the option to adjust the Compression Level for Concentrators on ESA. To enable compression, select the **Compression** checkbox. You can set the **Compression Level** for a Concentrator from 0-9:
- Compression Level = **0** (If compression is enabled, it allows Core Services to control the amount of compression.)
  - Compression Level = **1** (It uses the lowest amount of compression and has the highest performance.)
  - Compression Level = **9** (It uses the highest amount of compression and has the worst performance.)

Somewhere in the middle between 1 and 9 is usually the best setting, which is what you get when you select a compression level of 0. For more detailed information, see the *Core Database Tuning Guide*.

**Note:** When you set the compression level for a Concentrator on ESA, it sets the same compression level for that Concentrator for ESA Correlation Rules.


9. Click **Test Configuration** to make sure that it can communicate with the ESA service.
10. Click **Save**.

After you configure your data sources and they appear in the Available Configured Data Sources dialog, you can use them for your deployment.

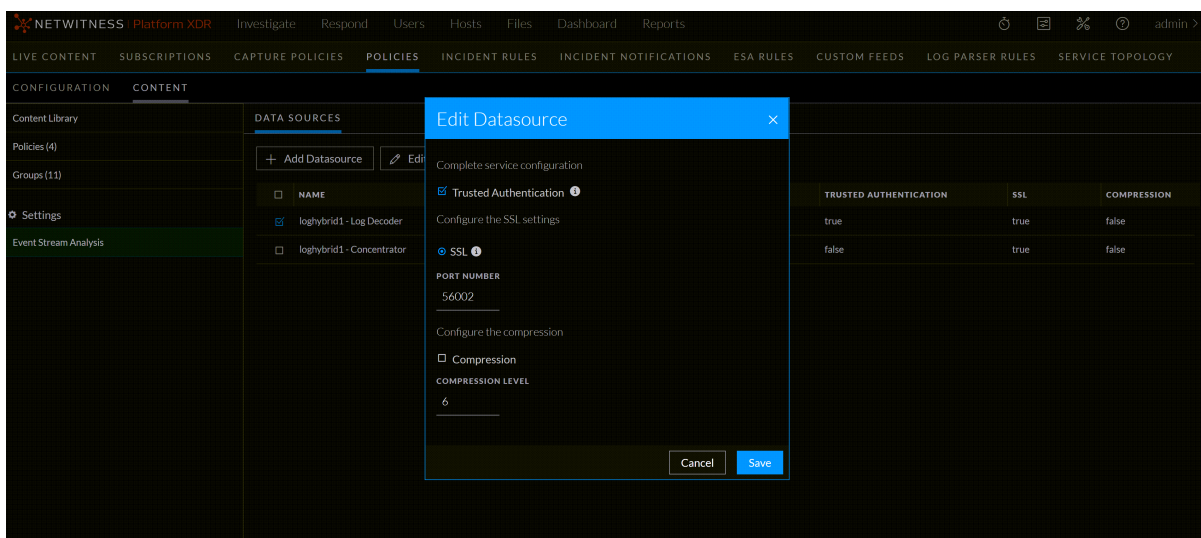
## Edit an ESA Datasource

You can edit the properties of the datasource at any point in time. You can edit the user credentials, SSL, port, and compression value of the datasource. When a data source password changes, it is important to change the password on the data source so that ESA can continue to communicate with the data source.

### To edit an ESA Datasource

1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.
3. Under **Settings**, click **Event Stream Analysis** > **Data Sources**.
4. Select a datasource and click **Edit Datasource**.

The Edit Datasource dialog is displayed.




5. Make the required changes in the datasource.
6. Click **Save**.

### Delete an ESA Datasource

You can delete one or more ESA datasources. Once the datasource is deleted, the service will be removed from the available configured list.

#### To delete an ESA Datasource

1. Go to  (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. Under **Settings**, click **Event Stream Analysis** > **Data Sources**.
4. Select a datasource and click **Delete Datasource**.  
A confirmation pop-up is displayed.
5. Click **Delete Datasource**.

### Manage Deployments

The ESA deployment consists of a policy with ESA rules, ESA services, and data sources. The ESA service scans your network for suspicious activity whenever you deploy policies. An ESA rule detects a different event every time, such as when a user account is created and deleted within 24 hours.

In addition, you can perform other steps on your deployment, such as changing a data source, editing or deleting a rule from the deployment through policy, renaming or deleting the deployment, or showing updates to the deployment, see [Additional ESA Correlation Rules Procedures](#)

In 12.1 and later versions, you must create a policy with the ESA rule content type and associate the policy with the group having a correlation service to create a deployment.

For more information on policies, see [Policies](#)

For more information about groups, see [Groups](#)

**Note:** With the unified ESA Deployments tab, you can manage deployments from a single view across all policies within Policy-based Centralized Content Management (CCM).

You can do the following:

- [View a Deployment](#)
- [Create a Deployment](#)
- [Edit a Deployment](#)
- [Start a Deployment](#)
- [Remove a Deployment](#)
- [Stop a Deployment](#)
- [Migrate ESA Deployments to Policies and Groups](#)

## View a Deployment

In the ESA deployment view, you can view a list of all the deployments associated with the policies and the actions you can perform with them. It helps you manage and set-up deployments within CCM to create, edit, deploy, remove, and stop deployments. NetWitness Platform XDR provides two methods to manage deployments.

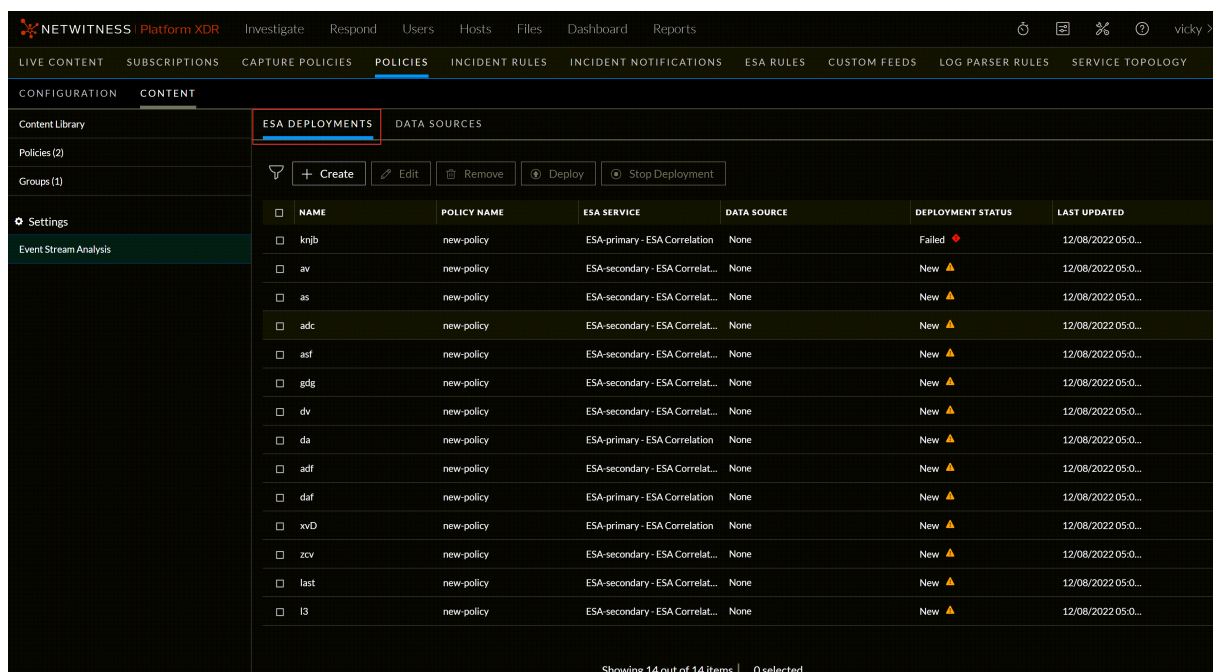
You can view deployments in the following ways:

- Using the **ESA Deployments** tab. The ESA Deployments tab provides a consolidated view of all the available deployments within CCM. You can create, edit, remove, and pause deployments.
- Using a specific policy. In this method, you cannot view other deployments. You need to go to each policy and create, edit, remove and pause a deployment.

### To view all deployments using the ESA Deployments tab

1. Go to  (CONFIGURE) > Policies > Content.
2. Under Settings, click Event Stream Analysis > ESA Deployments.

The available deployments are displayed.



## To view a deployment from a selected policy

1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.


The available policies are displayed.

3. Click a Policy.

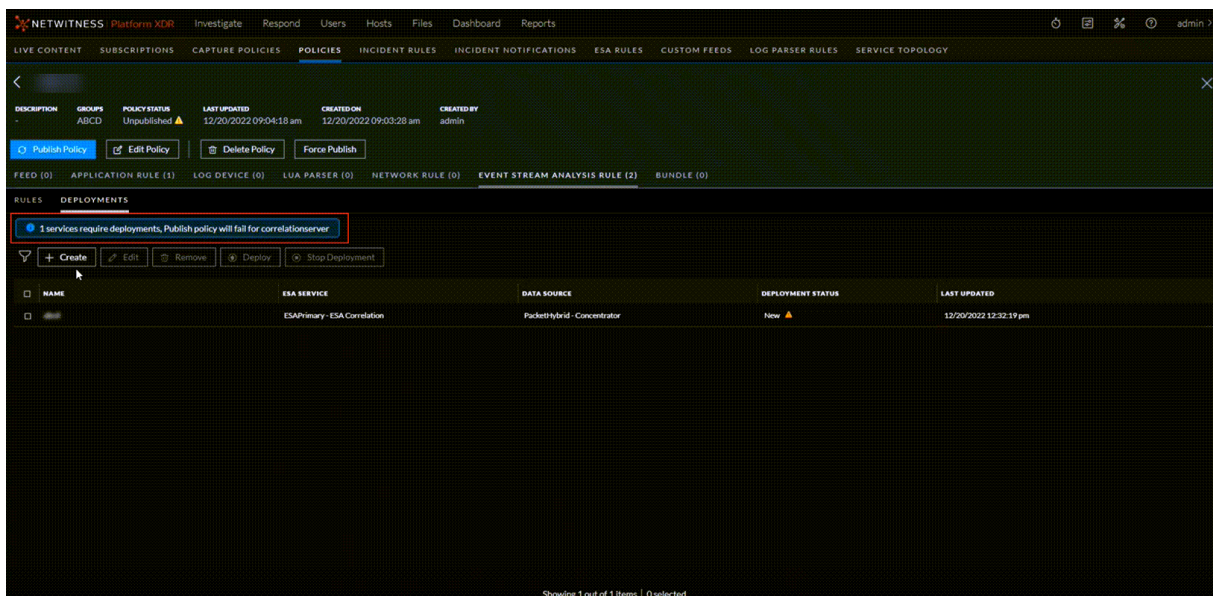
The selected policy view is displayed, and the Application Rule is default selected.

4. Click **Event Stream Analysis Rule** > **Deployments**.

The available deployments for the selected policy are displayed.

**Caution:** An icon  is displayed in the deployments view indicating services require deployments, publish policy will fail for correlation servers. You may need to create deployments for such services if required.





## Create a Deployment

When you create a deployment, you need to select a policy, ESA service, and data sources. An ESA rule deployment consists of an ESA service, one or more data sources, and a set of ESA rules. When you deploy rules, the ESA service runs them to detect suspicious or undesirable activity in your network. Each ESA rule detects a different event, such as when a user account is created and deleted within one hour.

For more information on data sources, see [Data Source](#)

In 12.1 and later versions, you must create a policy with the ESA rule content type and associate the policy with the group having a correlation service to create a deployment.

For more information on policies, see [Policies](#)

You can create deployments in the following ways:


- Using the ESA Deployments tab. The ESA Deployments tab provides a consolidated view of all the available deployments within CCM. You can create deployments.
- Using a specific policy. In this method, you cannot view other deployments. You need to go to each policy and create a deployment.

## Prerequisites

- The group is assigned to a policy.
- The Correlation server service is available in the groups assigned.
- A minimum of one ESA rule is added to the policy.
- ESA data source must be configured.

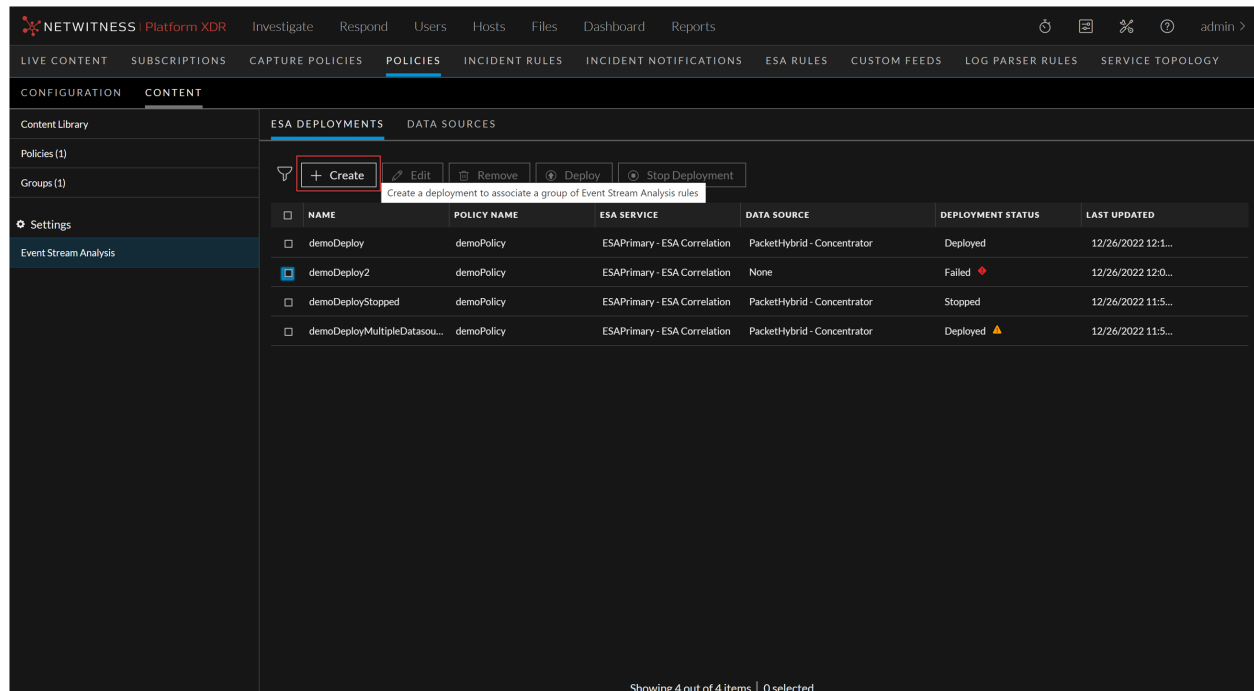
For more information about groups, see [Groups](#)

### To create a deployment using the ESA Deployments tab

1. Go to  (CONFIGURE) > Policies > Content.
2. Under Settings, click Event Stream Analysis > ESA Deployments.

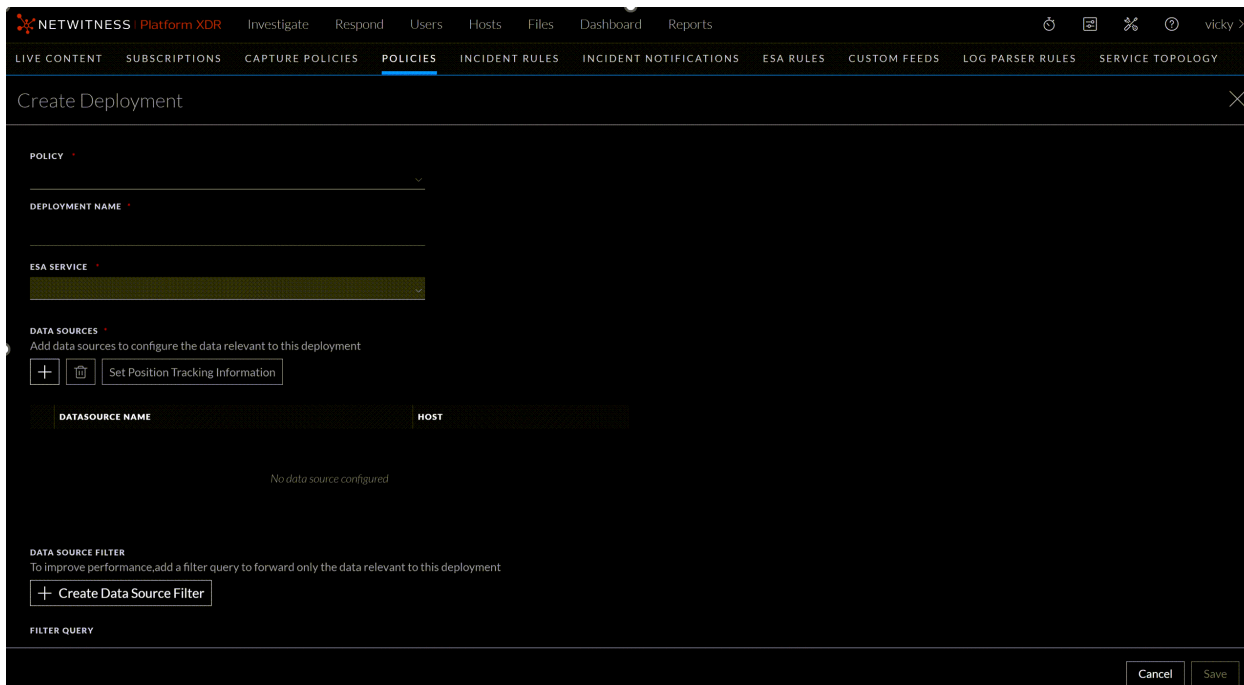
The available deployments are displayed.

3. Click + Create



NAME	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	LAST UPDATED
demoDeploy	demoPolicy	ESAPrimary - ESA Correlation	PacketHybrid - Concentrator	Deployed	12/26/2022 12:1...
demoDeploy2	demoPolicy	ESAPrimary - ESA Correlation	None	Failed	12/26/2022 12:0...
demoDeployStopped	demoPolicy	ESAPrimary - ESA Correlation	PacketHybrid - Concentrator	Stopped	12/26/2022 11:5...
demoDeployMultipleDatasou...	demoPolicy	ESAPrimary - ESA Correlation	PacketHybrid - Concentrator	Deployed	12/26/2022 11:5...

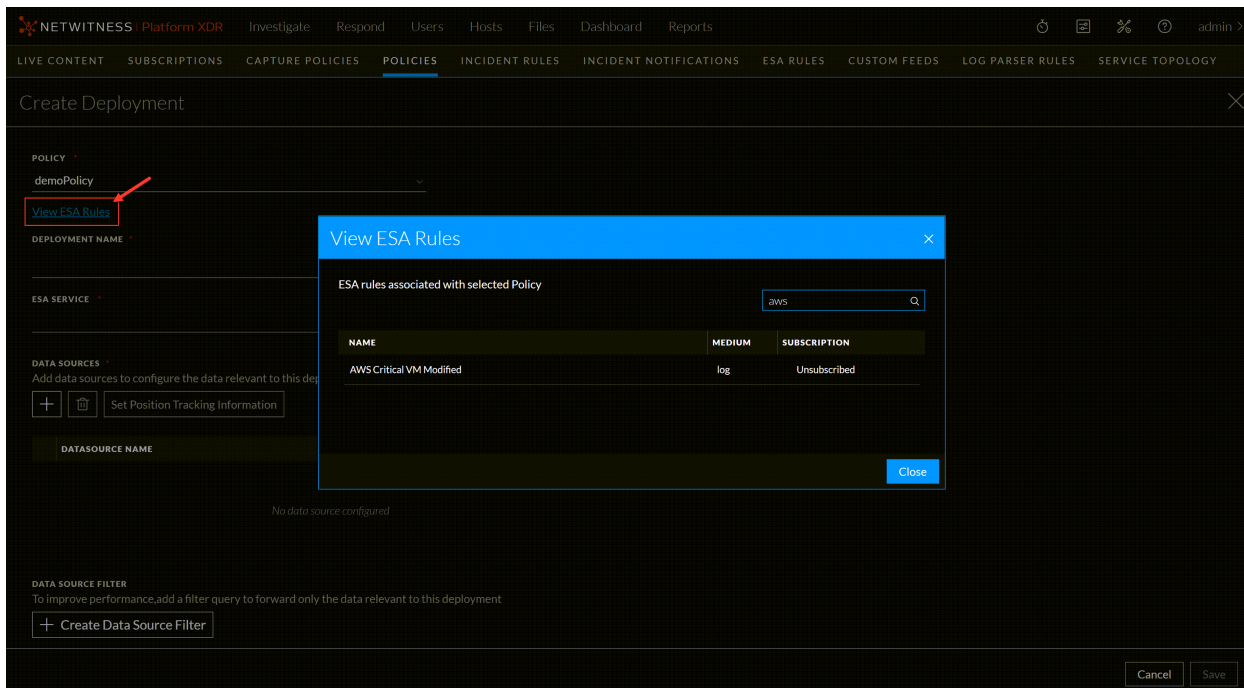
The Create Deployment dialog is displayed.



4. Select an eligible policy from the policy list.

**Note:** All the policies that meet the criteria mentioned above are listed in the policy drop-down. It is required to select a policy to proceed further.

If required, you can click on View ESA Rules to search for rules associated with selected policy.

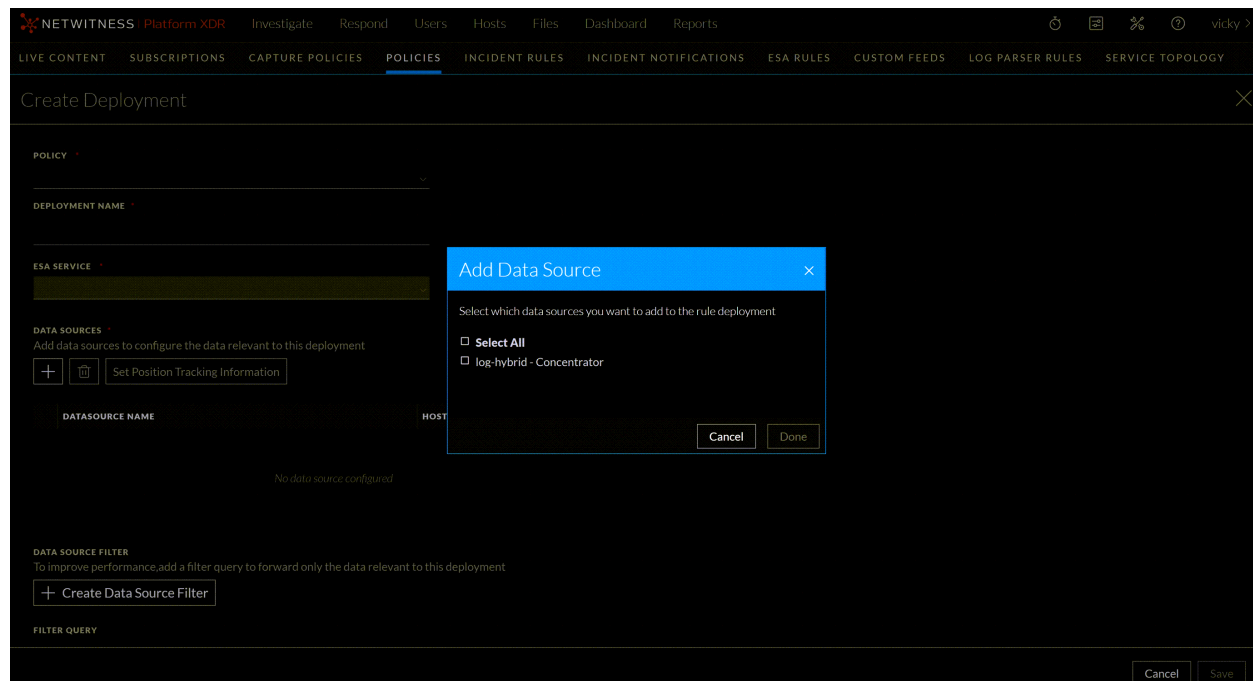


5. Enter a name for the deployment.
6. Select a service from the **ESA Service** drop-down list.

**Note:** Once the deployment is saved, the selected policy, name and ESA service cannot be modified.


7. Under **Data Sources**, click + to add a data source.

The **Add Data Source** dialog is displayed.

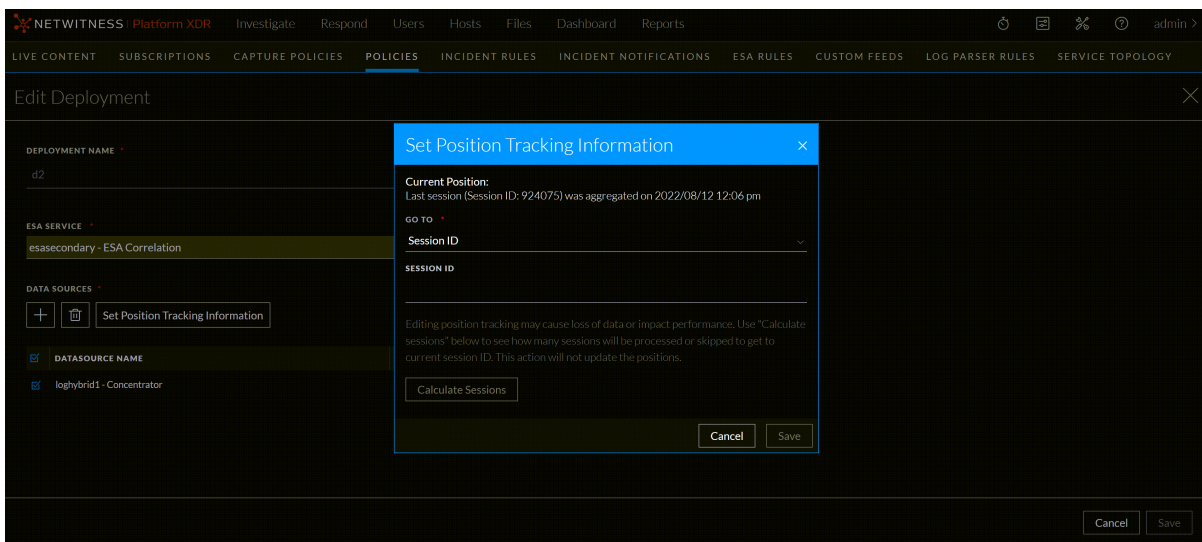


8. Select one or more data sources and click Done.

**IMPORTANT:** If the data sources are not listed, you can add the required datasource. For more information, see the topic [Add an ESA Datasource](#).

9. To delete the data source, select the data source and click .
10. (Optional) Select the required data source and click **Set Position Tracking Information** to process specific or ignore certain sessions.

The **Set Position Tracking Information** dialog is displayed.



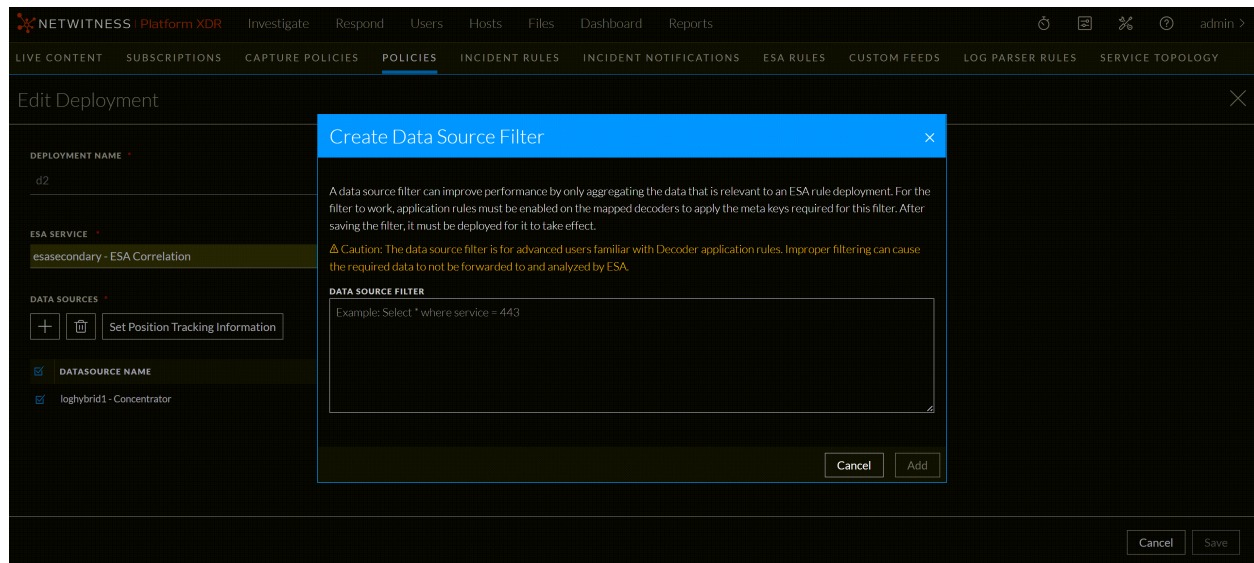
- a. In the Position Tracking Information dialog, perform the following:
  - i. If you want to set the position tracking information based on date and time stamp:  
In the **Go To** drop-down menu, select **Date and Time** and enter the date and time.
  - ii. If you want to set the position tracking information, based on the session ID:  
In the **Go To** drop-down menu, select **Session ID** and enter the session ID in the **Session ID** field.  
  
The ESA Correlation service starts processing the events from the session ID that you entered.
- b. Click **Calculate Sessions** to calculate the number of sessions that will be processed to the existing position of the data source, if any.
- c. To save the edited position tracking data source, click **Save**.

For more information on Position Tracking Information, see [Appendix B: Position Tracking Information](#).

11. (Optional) To filter out specific session data coming into ESA, under Data Source Filter, click + **Create Data Source Filter**.

**Caution:** The data source filter is for advanced users familiar with Decoder application rules. Improper filtering can cause the required data not to be forwarded to and analyzed by ESA.

The **Create Data Source Filter** dialog is displayed.



a. Specify the filter query in the below format as shown in the following example:

**Select \*where service = 443**

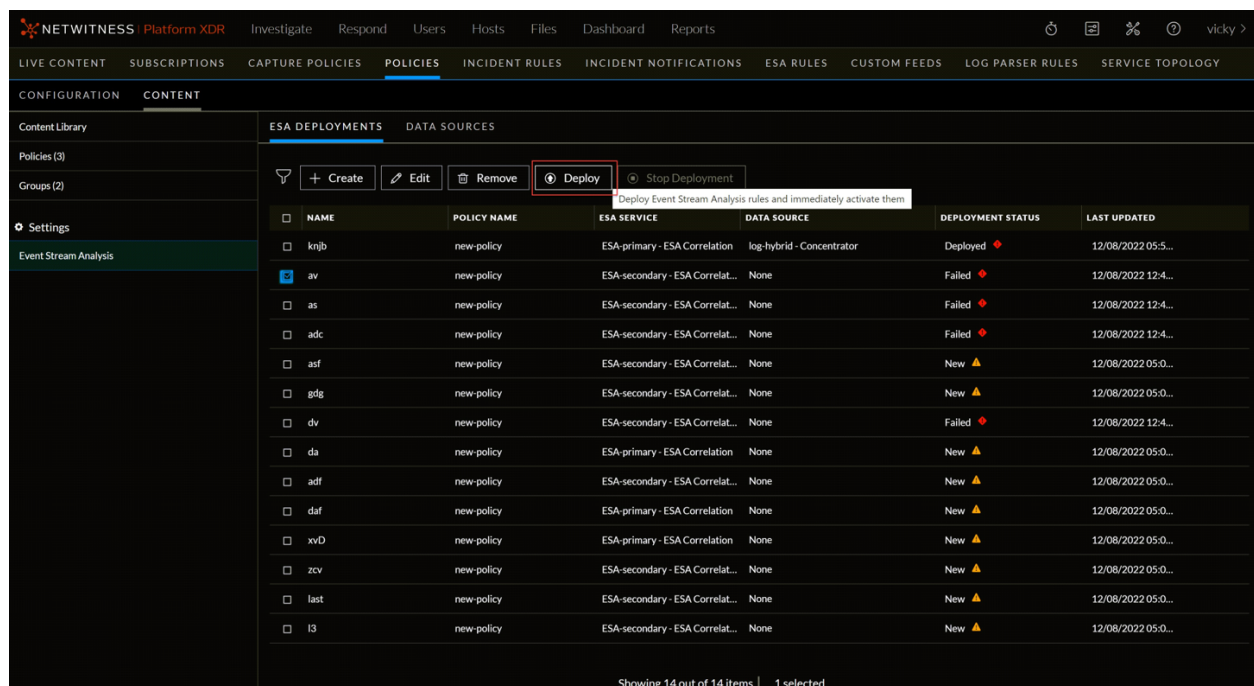
Based on the query processed, it will filter out only HTTPS logs-related sessions and will be forwarded to the ESA.

b. Click **Add**.


c. If you want to delete the existing data sources filter, click **Clear Data Source Filter**, and **Save** to remove it permanently.

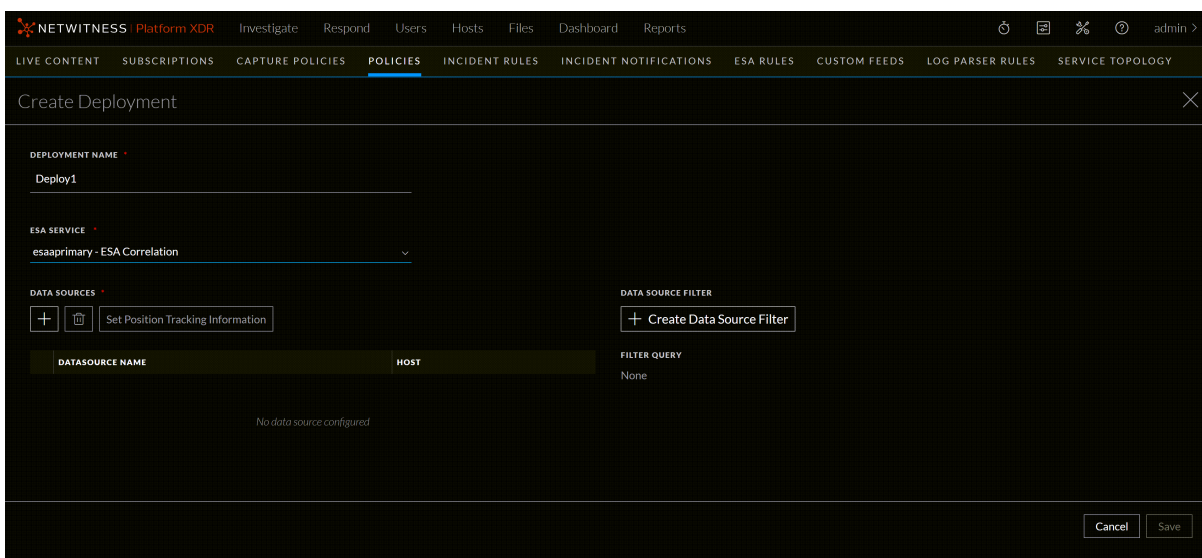
12. To save the deployment, click **Save**.

13. Select the created deployment and click **Deploy**.




### To create a deployment from a selected policy

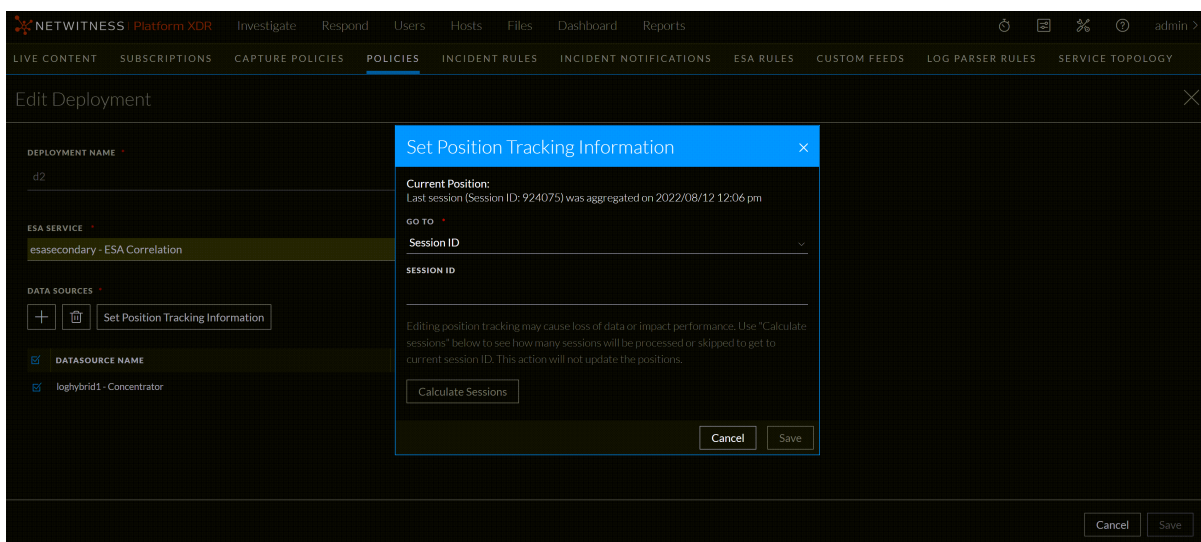
1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.  
The available policies are displayed.
3. Click a Policy.  
The selected policy view is displayed and by default **Application Rule** is selected.
4. Click **Event Stream Analysis Rule** > **Deployments**.  
The available deployments for the selected policy are displayed.
5. Click **+ Create Deployment**.  
The Create Deployment dialog is displayed.



6. Enter a name for the deployment.
7. Select a service from the **ESA Service** drop-down list.
8. Under **Data Sources**, click + to add a data source.  
The Add Data Source dialog is displayed.
9. Select one or more data sources and click **Done**.

**IMPORTANT:** If the data sources are not listed, you can add the required datasource. For more information, see the topic [Add an ESA Datasource](#).

10. To delete the data source, select the data source and click .
11. (Optional) the required data source and click **Set Position Tracking Information** to reprocess specific sessions or ignore certain sessions.  
The Set Position Tracking Information dialog is displayed.



- a. In the Position Tracking Information dialog, perform the following:
  - i. If you want to set the position tracking information based on date and time stamp:  
In the **Go To** drop-down menu, select **Date and Time** and enter the date and time.
  - ii. If you want to set the position tracking information, based on the session ID:  
In the **Go To** drop-down menu, select **Session ID** and enter the session ID in the **Session ID** field.  
  
The ESA Correlation service starts processing the events from the session ID that you entered.
- b. Click **Calculate Sessions** to calculate the number of sessions that will be processed with respect to the existing position of the data source, if any.
- c. To save the edited position tracking data source, click **Save**.
- d. The tracking position information will be deployed to the ESA Correlation service, only when the deployment is successfully completed.

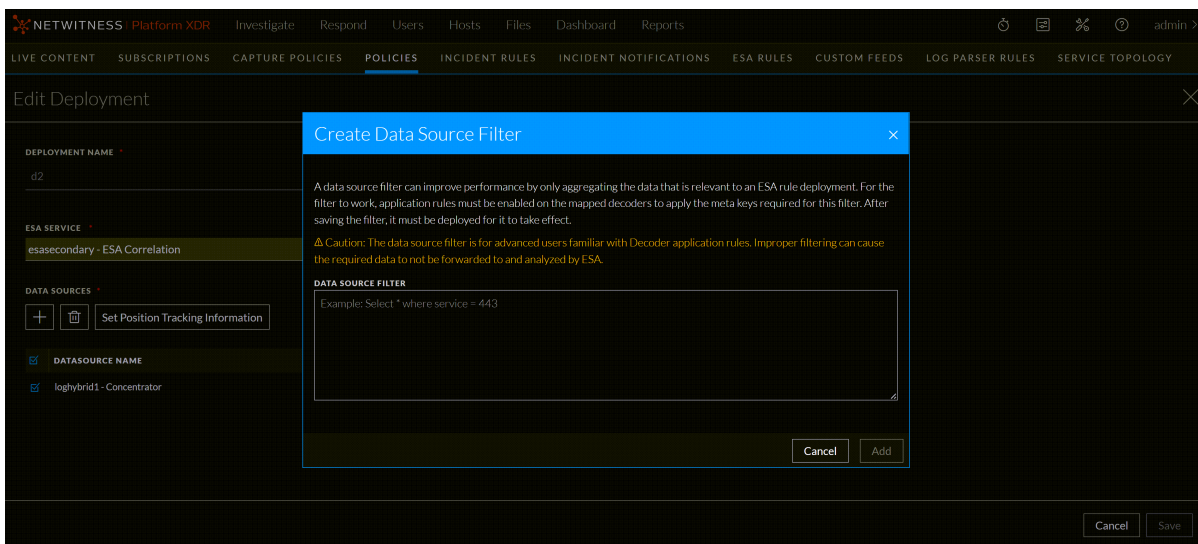
For more information on Position Tracking Information, see [Appendix B: Position Tracking Information](#).

12. (Optional) To filter out certain session data coming into ESA, under Data Source Filter, click + **Create Data Source Filter**.

**Caution:** The data source filter is for advanced users familiar with Decoder application rules. Improper filtering can cause the required data to not be forwarded to and analyzed by ESA.

The Create Data Source Filter dialog is displayed.





- a. Specify the filter query in the below format as shown in the following example:  
**Select \*where service = 443**  
 Based on the query processed, it will filter out only HTTPS logs related sessions and will be forwarded to the ESA.
  - b. Click **Add**.
  - c. If you want to delete the existing data sources filter, click **Clear Data Source Filter** and click **Save** to remove it permanently.
13. To save deployment, click **Save**.
  14. Select the created deployment and click **Deploy**.

## Edit a Deployment

You can edit a deployment to change the data source, create a data source filter, and view ESA rules that are associated with this deployment. A data source filter can improve performance by only aggregating the data that is relevant to an ESA rule deployment. For the filter to work, application rules must be enabled on the mapped decoders to apply the meta keys required for this filter. After saving the filter, it must be deployed for it to take effect.

However, you cannot change the deployment name, or ESA service that are associated with the deployment.

NetWitness Platform XDR provides two methods to manage deployments.

You can edit deployments in the following ways:

- Using the ESA Deployments tab. The **ESA Deployments** tab provides a consolidated view of all the available deployments within CCM. You can edit deployments.
- Using a specific policy. In this method, you cannot view other deployments. You need to go to each policy and edit a deployment.

### To edit a deployment from the ESA Deployments tab

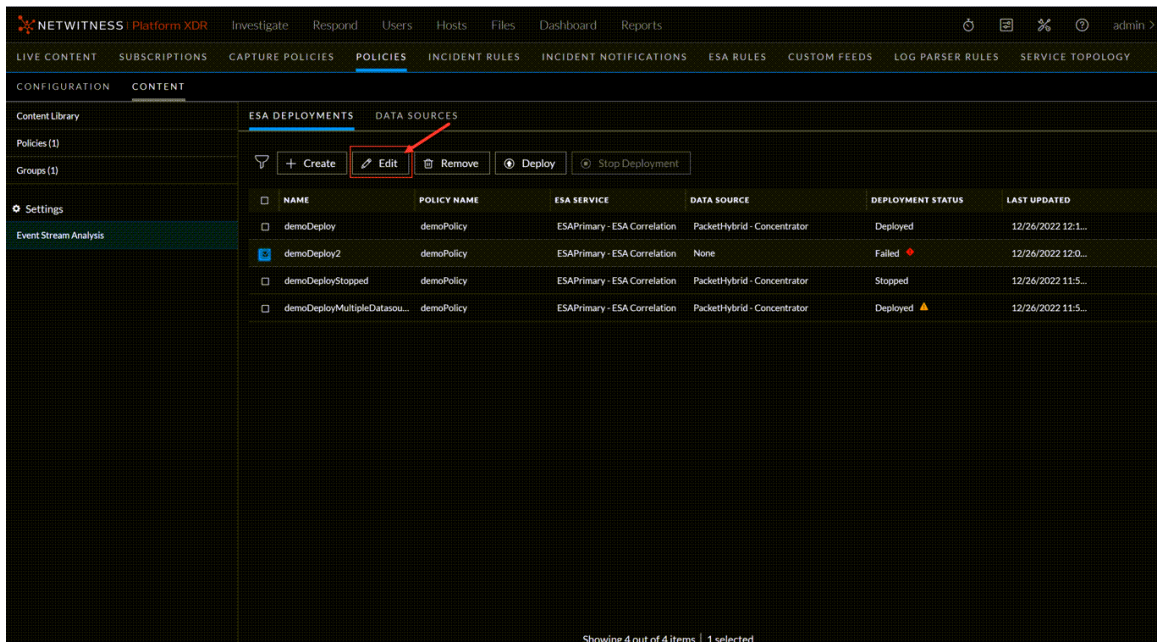
1. Go to  (CONFIGURE) > Policies > Content.

2. Under **Settings**, click **Event Stream Analysis > ESA Deployments**.

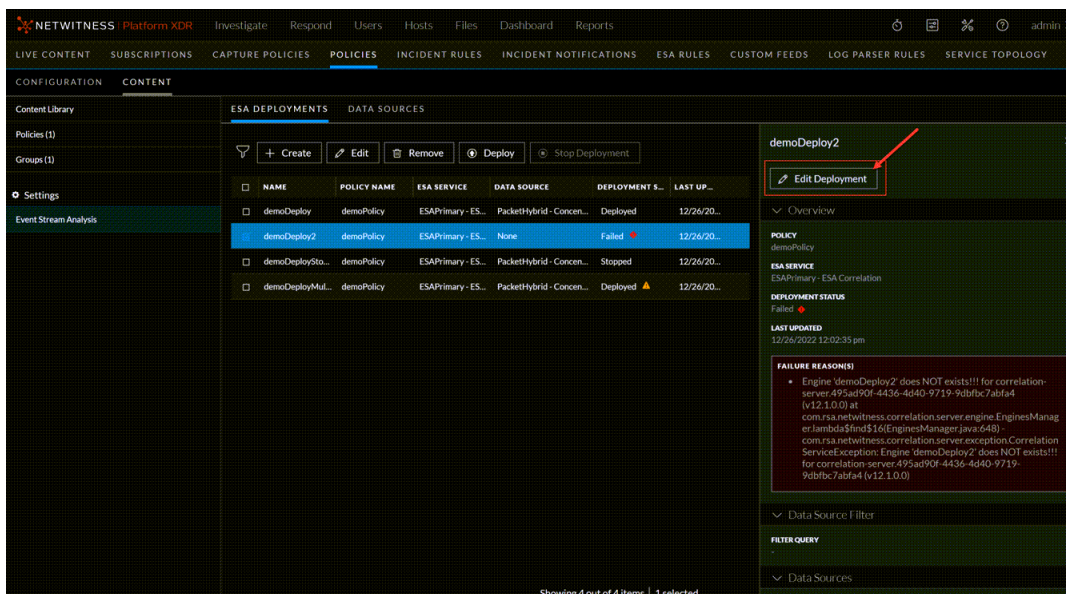
The available deployments are displayed.

3. Select a deployment and click **Edit** or **Edit Deployment**.

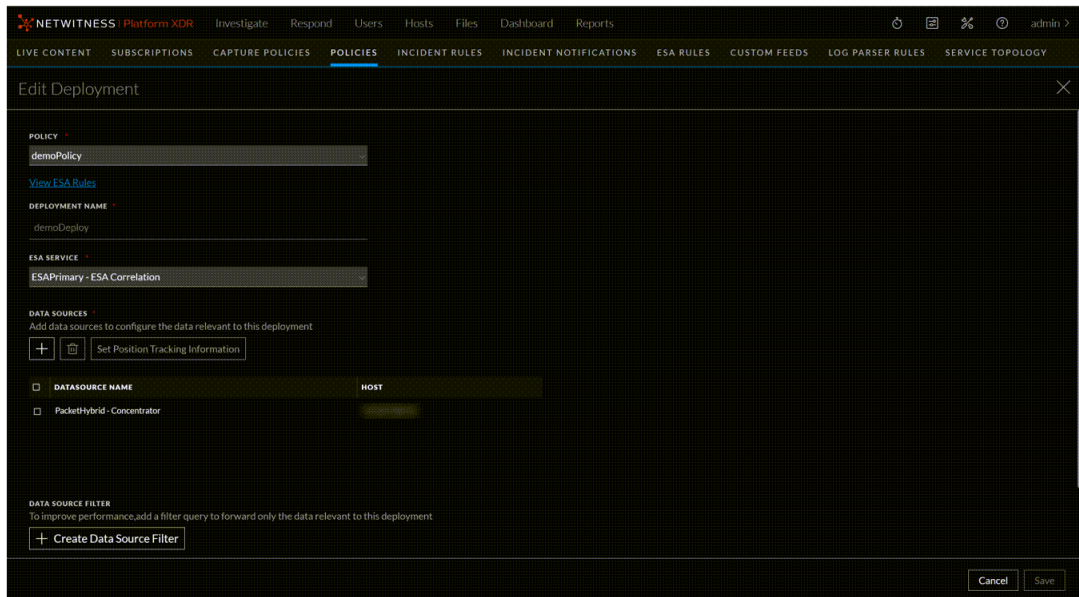
- a. When you select the checkbox and click **Edit**.



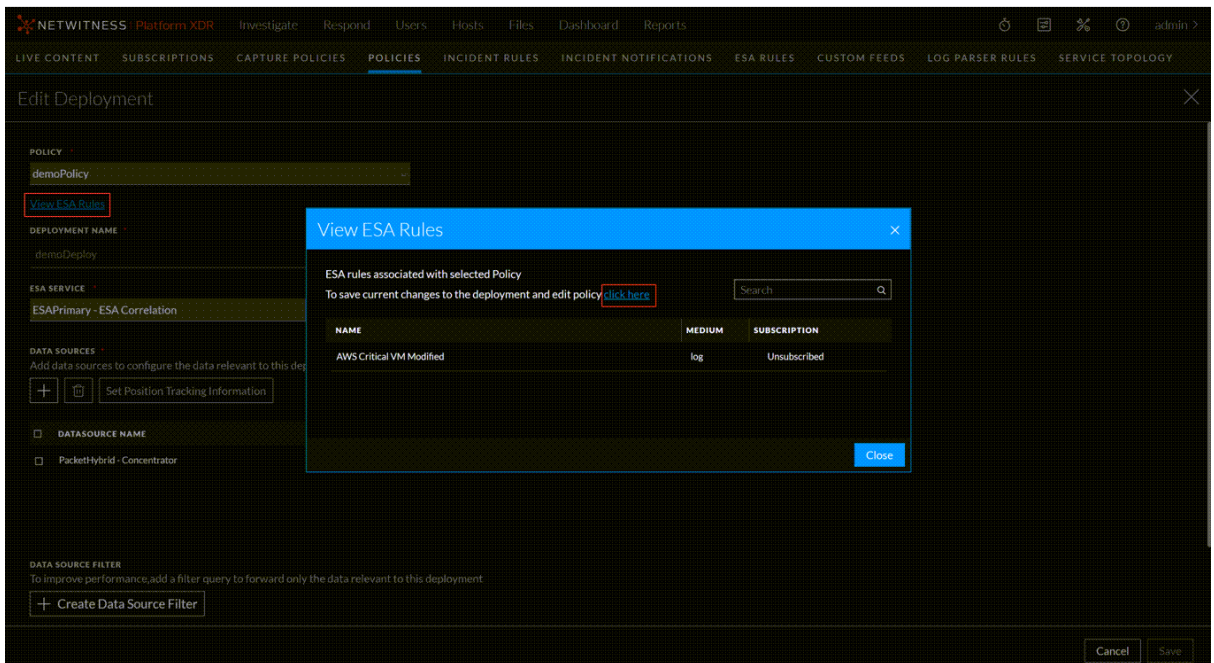
- b. When you select or click a row of the deployment, a right panel is displayed to click **Edit Deployment**.



The **Edit Deployment** dialog is displayed.




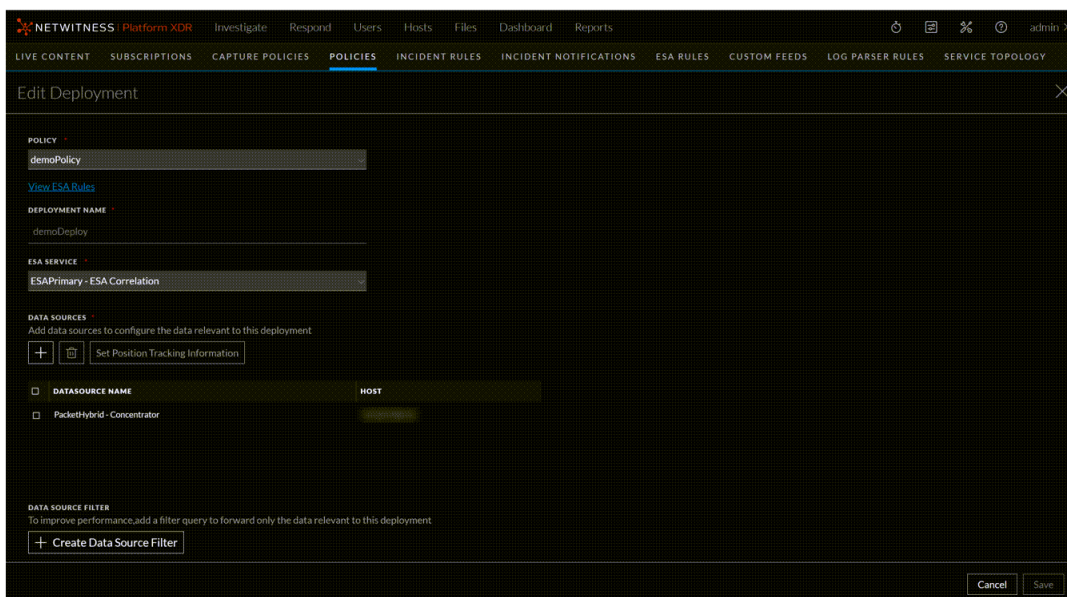
- (Optional) you can click on **View ESA Rules** to search for rules associated with selected policy. To save current changes to the deployment and modify the policy, select **click here** and navigate to the **Edit Content Policy** page.



- Make the required changes in the deployment.  
Policy, deployment name, and ESA service are pre-populated and cannot be modified.
- Click **Save**.
- Select the deployment and click **Deploy**.

## To edit a deployment from a selected policy

1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.  
The available policies are displayed.
3. Click a Policy.  
The selected policy view is displayed and by default **Application Rule** is selected.
4. Click **Event Stream Analysis Rule** > **Deployments**.  
The available deployments for the selected policy are displayed.
5. Select a deployment to edit and click **Edit Deployment**.  
The **Edit Deployment** dialog is displayed.



6. Make the required changes in the deployment.
7. Click **Save**.
8. Select the deployment and click **Deploy**.

**Note:** You can deploy the changes either by performing a **Deploy** action on selected deployment or by publishing the policy. Publishing a policy with deployment in stopped state, will not deploy the deployment.

## Start a Deployment

The deployment includes ESA services with policy and associated ESA rules. When you initiate deployment, the correlation services start processing sessions from the configured data sources for matching events for the selected ESA rules in the policy.

For more information about ESA services and rules, see [Alerting with ESA Correlation Rules](#)

You can start deployments in the following ways:

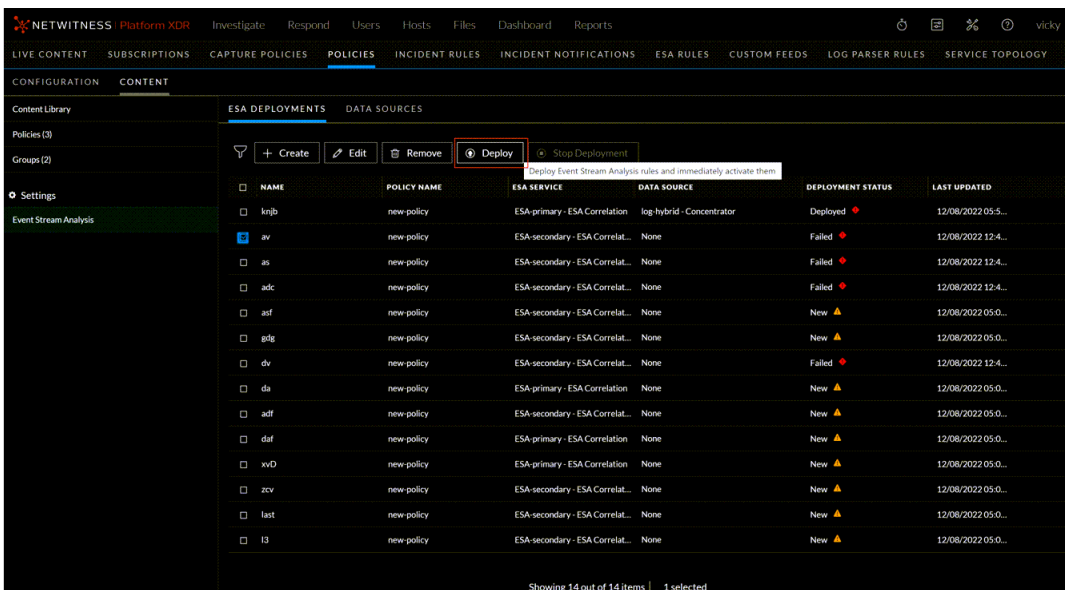
- Using the ESA Deployments tab. The ESA Deployments tab provides a consolidated view of all the available deployments within CCM. You can initiate deployments.
- Using a specific policy. In this method, you cannot view other deployments. You need to go to each policy and initiate a deployment.

### To initiate a deployment, with the ESA Deployments tab

1. Go to  (CONFIGURE) > Policies > Content.
2. Under Settings, click Event Stream Analysis > ESA Deployments.


The available deployments are displayed.

3. Select a deployment and click **Deploy**.



NAME	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	LAST UPDATED
knjb	new-policy	ESA-primary - ESA Correlation	log-hybrid - Concentrator	Deployed	12/08/2022 05:5...
zv	new-policy	ESA-secondary - ESA Correlat...	None	Failed	12/08/2022 12:4...
as	new-policy	ESA-secondary - ESA Correlat...	None	Failed	12/08/2022 12:4...
adc	new-policy	ESA-secondary - ESA Correlat...	None	Failed	12/08/2022 12:4...
asf	new-policy	ESA-secondary - ESA Correlat...	None	New	12/08/2022 05:0...
gls	new-policy	ESA-secondary - ESA Correlat...	None	New	12/08/2022 05:0...
dv	new-policy	ESA-secondary - ESA Correlat...	None	Failed	12/08/2022 12:4...
da	new-policy	ESA-primary - ESA Correlation	None	New	12/08/2022 05:0...
adf	new-policy	ESA-secondary - ESA Correlat...	None	New	12/08/2022 05:0...
daf	new-policy	ESA-primary - ESA Correlation	None	New	12/08/2022 05:0...
xvD	new-policy	ESA-primary - ESA Correlation	None	New	12/08/2022 05:0...
zcv	new-policy	ESA-secondary - ESA Correlat...	None	New	12/08/2022 05:0...
last	new-policy	ESA-secondary - ESA Correlat...	None	New	12/08/2022 05:0...
l3	new-policy	ESA-secondary - ESA Correlat...	None	New	12/08/2022 05:0...

### To start a deployment with selected policy

1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.  
The available policies are displayed.
3. Click a Policy.  
The selected policy view is displayed and by default **Application Rule** is selected.
4. Click **Event Stream Analysis Rule** > **Deployments**.  
The available deployments for the selected policy are displayed.
5. Select the deployment to deploy and click **Deploy**.

**Note:** You can deploy the changes either by performing a Deploy action on selected deployment or by publishing the policy. Publishing a policy with deployment in stopped state, will not deploy the deployment.


## Remove a Deployment

You can delete one or more deployments when those deployments are not required. Once the deployment is deleted, all the configurations associated with the deployment will be permanently deleted from the correlation server. The alert process will be stopped for the deleted deployment.

You can remove deployments in the following ways:

- Using the **ESA Deployments** tab. The ESA Deployments tab provides a consolidated view of all the available deployments within CCM. You can remove deployments.
- Using a specific policy. In this method, you cannot view other deployments. You need to go to each policy and remove a deployment.

### To remove a deployment from the ESA Deployments tab

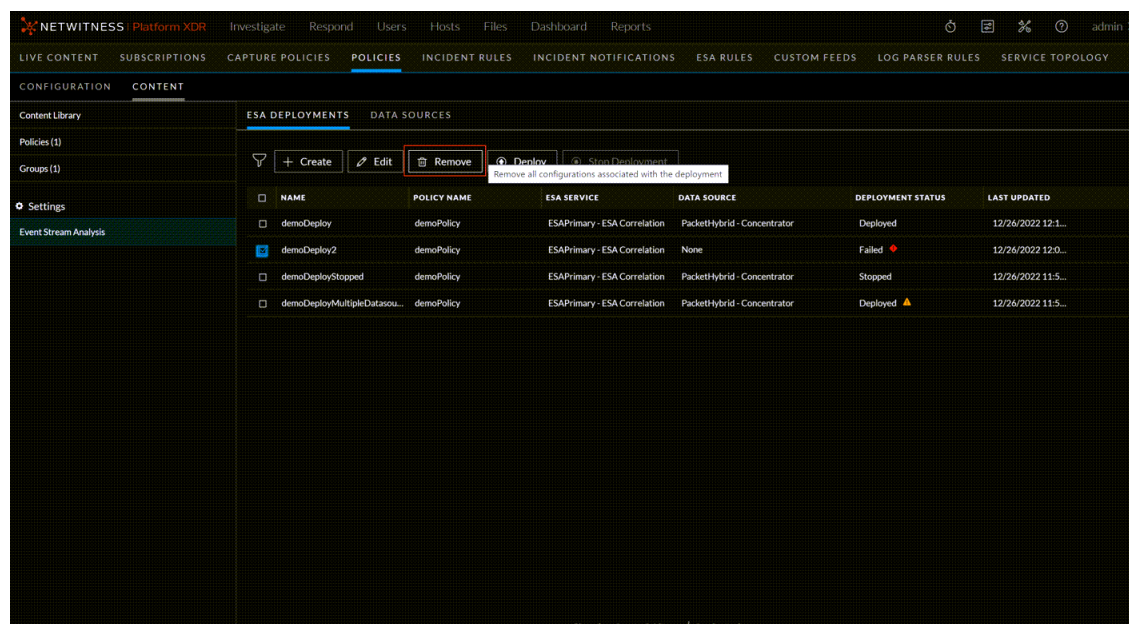
1. Go to  (CONFIGURE) > Policies > Content.
2. Under Settings, click Event Stream Analysis > ESA Deployments.

The available deployments are displayed.


3. Select the deployment that needs to be removed and click **Remove**.

A confirmation pop-up is displayed to confirm.

4. Click **Remove**.



### To remove a deployment from a selected policy

1. Go to  (CONFIGURE) > Policies.
2. In the policies panel, click **Content**.  
The available policies are displayed.
3. Click a Policy.

The selected policy view is displayed and by default **Application Rule** is selected.

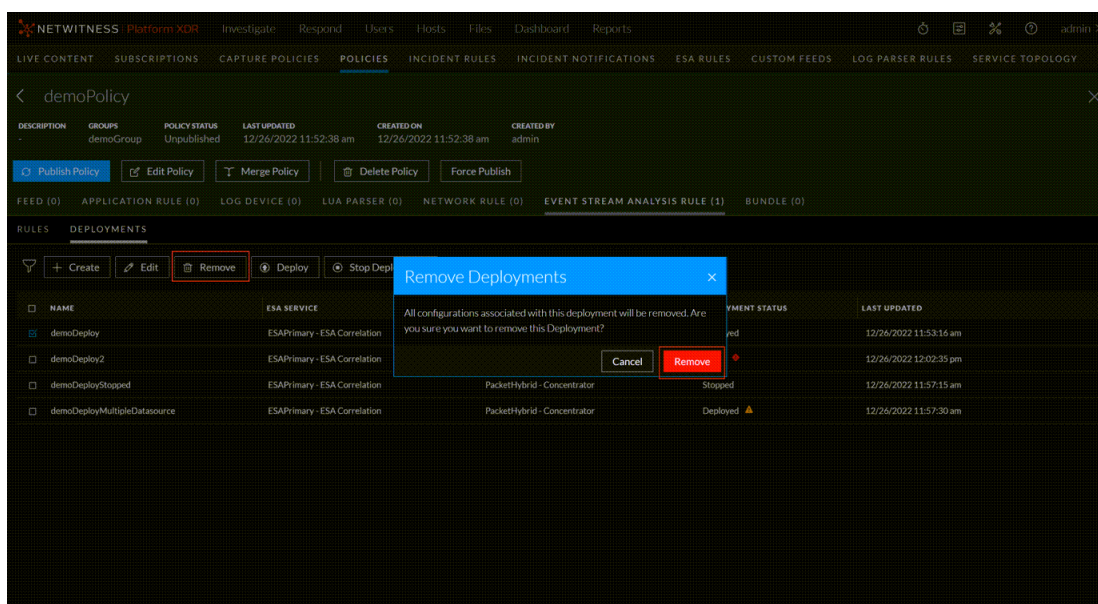
4. Click **Event Stream Analysis Rule > Deployments**.

The available deployments for the selected policy are displayed.

5. Select the deployment that needs to be removed and click **Remove Deployment**.

A confirmation pop-up is displayed to confirm if you want to remove it.

6. Click **Remove**.



**Note:** It is required to have at least one deployment associated with the correlation service present in the group associated with the policy.

## Stop a Deployment

You can stop a deployment to temporarily pause an ESA deployment. This will stop processing the event stream analysis alerts corresponding to the deployed policy.

To delete a deployment completely, see [Remove a Deployment](#)

To initiate a deployment again, see [Start a Deployment](#)

You can stop deployments in the following ways:

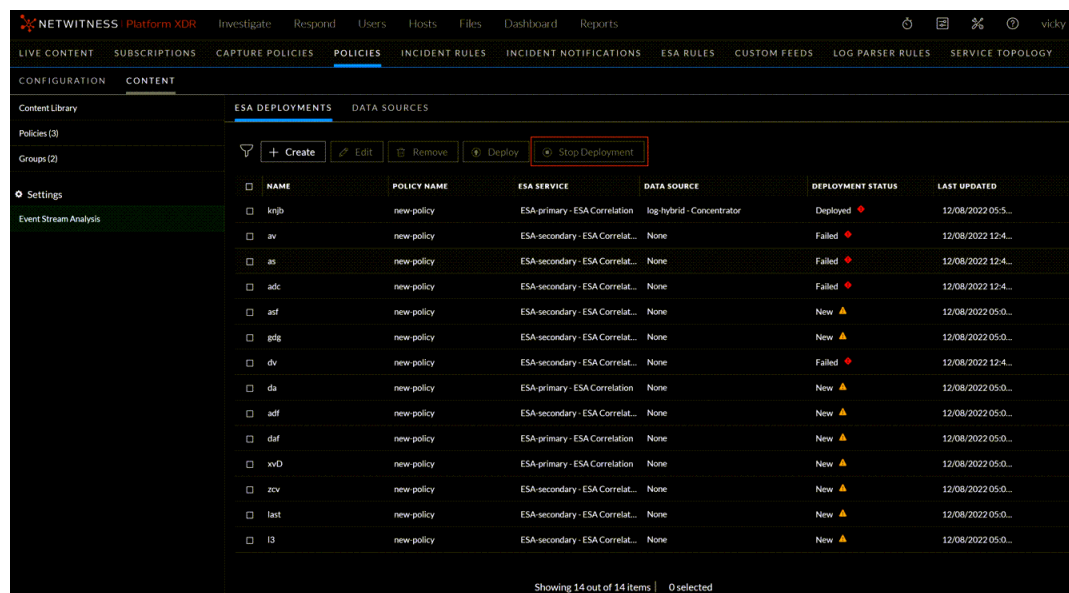
- Using the ESA Deployments tab. The ESA Deployments tab provides a consolidated view of all the available deployments within CCM. You can stop deployments.
- Using a specific policy. In this method, you cannot view other deployments. You need to go to each policy and stop a deployment.

### To stop a deployment from the ESA Deployments tab


1. Go to  (CONFIGURE) > Policies > Content.
2. Under **Settings**, click **Event Stream Analysis > ESA Deployments**.

The available deployments are displayed.

3. Select the deployment that must be stopped temporarily and click **Stop Deployment**.

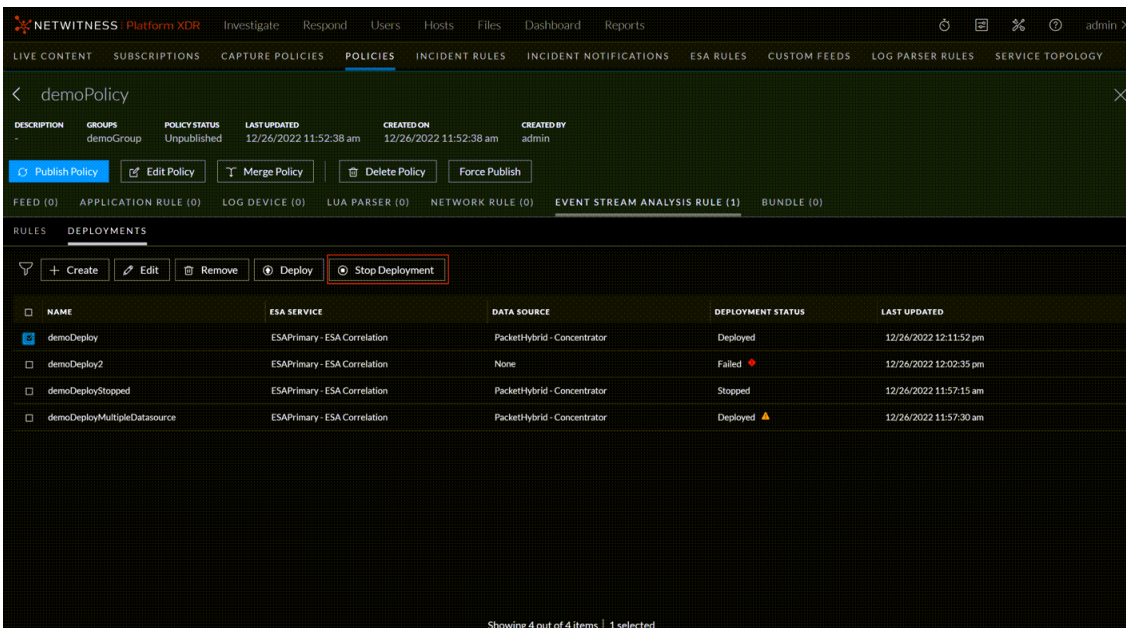


### To stop a deployment from a selected policy

1. Go to  (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.  
The available policies are displayed
3. Click a Policy.  
The selected policy view is displayed and by default **Application Rule** is selected.
4. Click **Event Stream Analysis Rule** > **Deployments**.  
The available deployments for the selected policy are displayed.
5. Select the deployment that needs to be stopped temporarily and click **Stop Deployment**.



**Note:** Publishing the policy will not deploy the stopped deployments.

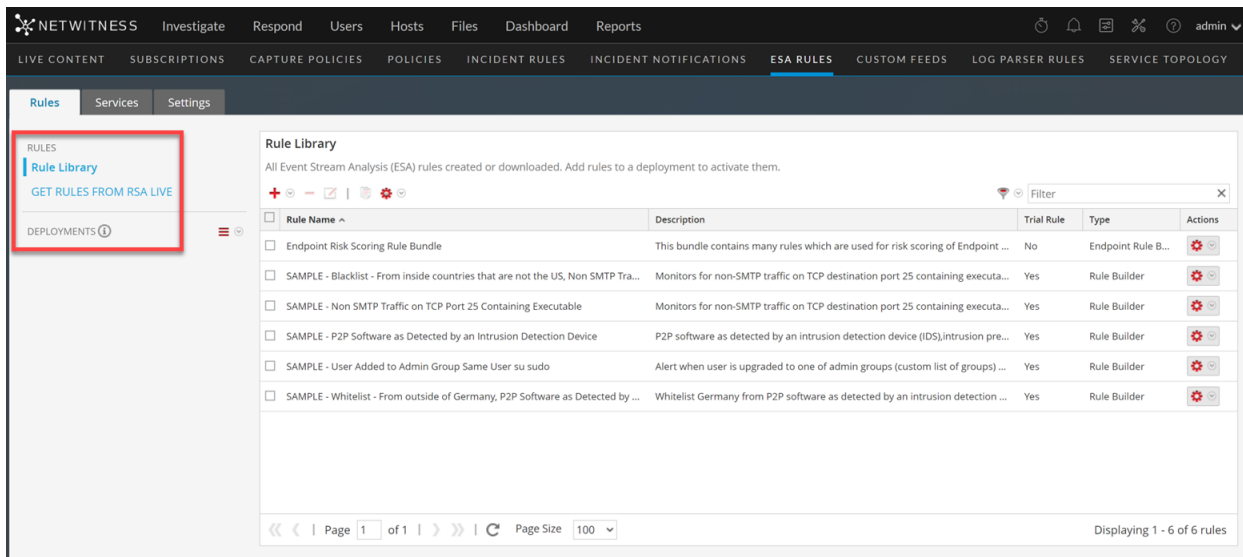


## Migrate ESA Deployments to Policies and Groups

From version 12.1 and later, on successful upgrade of the Admin Server, the ESA deployments are managed by the policies and groups page. The deployments are not available on **(CONFIGURE)** > **ESA Rules** page.

### 12.0 and Earlier version

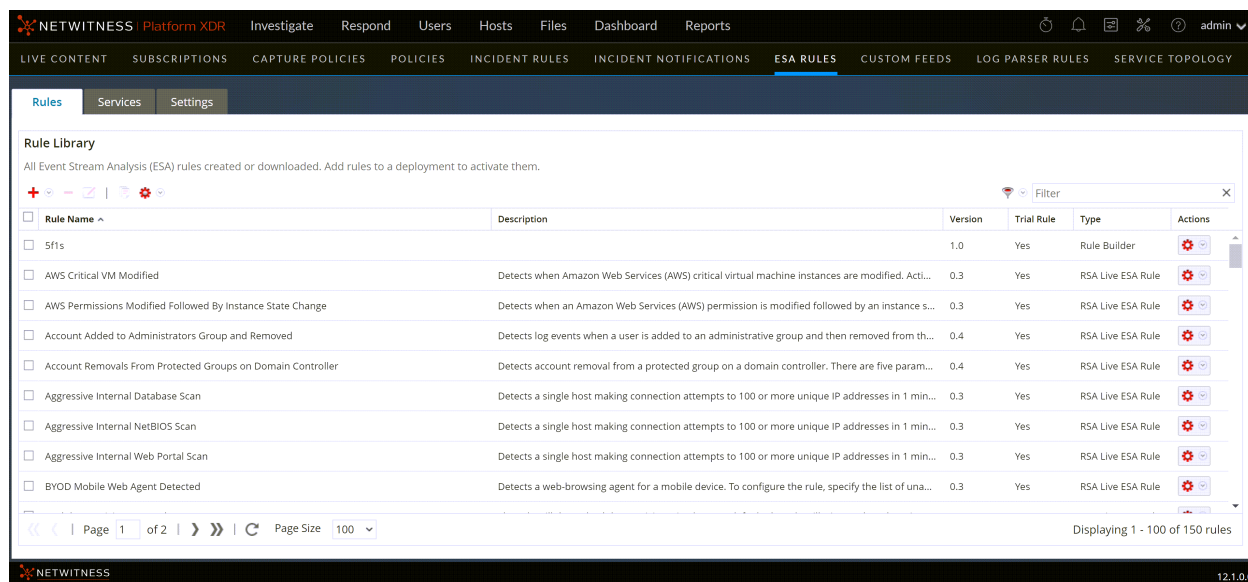
ESA Rules page in the 12.0 version.



### 12.1 version

Updated ESA Rules page in 12.1 version, where only rule libraries are available.

**Note:** The ESA deployments, after upgrading the Admin Server to 12.1 are not available to view or modify until the Correlation servers are also upgraded to the 12.1 version. However, the events are consumed, and ESA alerts are processed by the Correlation server.



All the deployments are automatically migrated to policies and groups:

- Each deployment is converted into a policy and a group.
- Once the ESA Correlation server is upgraded to the 12.1 version, you can access these deployments as groups and policies.

**IMPORTANT:** If there is any need to import ESA Rules and Enrichments. NetWitness recommends importing those missing rules and enrichments before the upgrade.

The following table provides the information on different deployment states for Policy and Groups:

SINo	Pre-upgrade Deployment State	Post-upgrade Deployment State		
		Creates Policy	Creates Group	The policy will be Published
1	Healthy deployment	Yes	Yes	Yes
2	Deployment with errors	Yes	Yes	Yes
3	Deployment with only rules	Yes	No	No
4	Deployment with no rules	No	No	No

Healthy deployment contains no errors, and the required resources such as ESA Server, Data source, and ESA rule are added.

**Note:** NetWitness recommends that all the deployments maintain an error-free state and also remove any unnecessary or unused ESA deployments.

## References

This section is a collection of references, which describe the user interface and more detailed information about how Policy-based Centralized Content Management works in NetWitness. The topics are presented in alphabetical order.

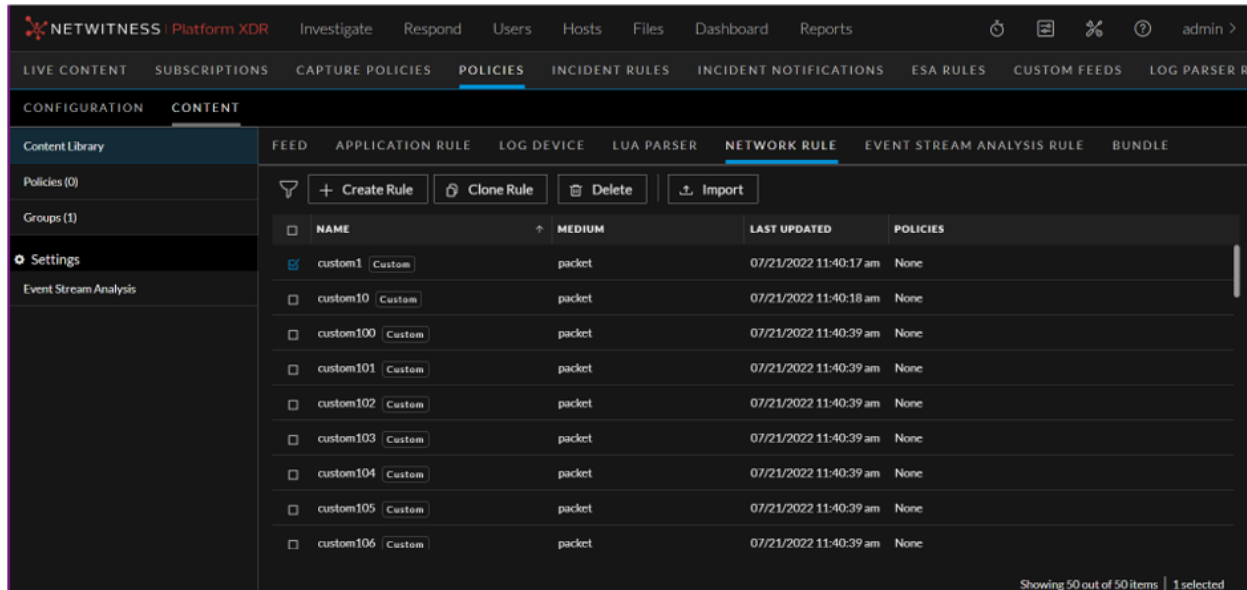
### Content Library Tab

The  (CONFIGURE) > **Policies** view contains two tabs: **Configuration** and **Content**.

The **CONTENT** tab has **Content Library**, **Policies** and **Groups** on the left panel.

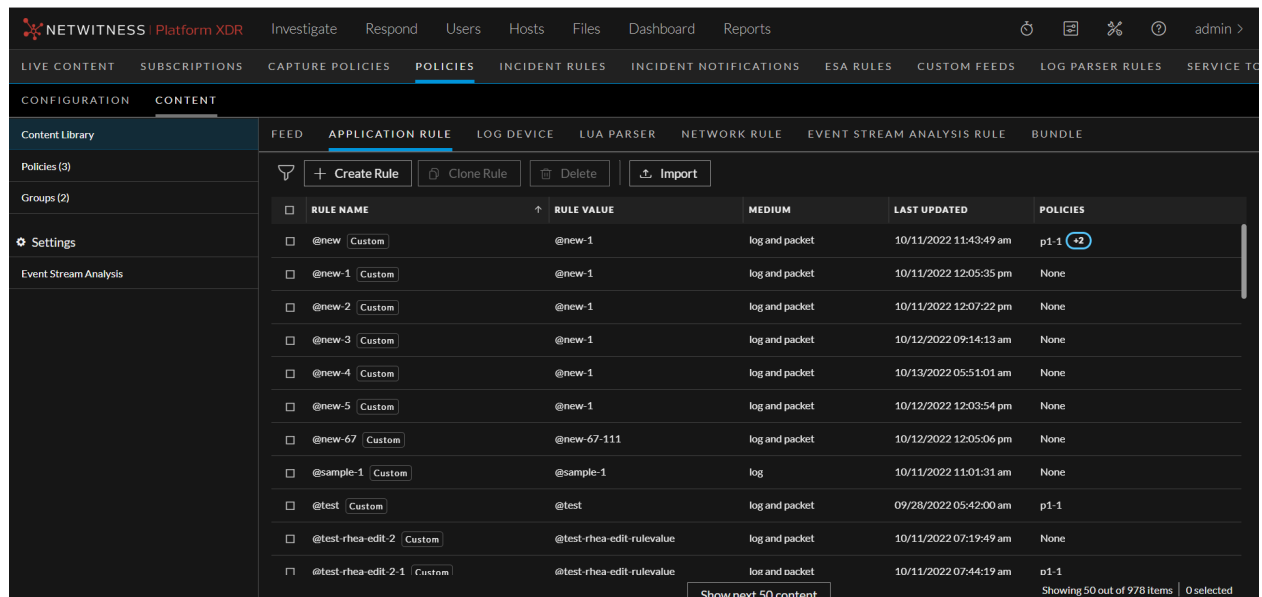
Below is an example of the **Content** > **Content Library** tab:

12.1 Version:



NAME	MEDIUM	LAST UPDATED	POLICIES
custom1 Custom	packet	07/21/2022 11:40:17 am	None
custom10 Custom	packet	07/21/2022 11:40:18 am	None
custom100 Custom	packet	07/21/2022 11:40:39 am	None
custom101 Custom	packet	07/21/2022 11:40:39 am	None
custom102 Custom	packet	07/21/2022 11:40:39 am	None
custom103 Custom	packet	07/21/2022 11:40:39 am	None
custom104 Custom	packet	07/21/2022 11:40:39 am	None
custom105 Custom	packet	07/21/2022 11:40:39 am	None
custom106 Custom	packet	07/21/2022 11:40:39 am	None

12.1.1 Version:




## 1 Toolbar

- Create Rule - Lets you create a rule.
- Clone Rule - Lets you clone an application rule or network rule. For more information, see [Clone Application Rule](#) or [Clone Network Rule](#).
- Delete - Lets you delete an application rule or network rule. For more information, see [Delete Application Rule](#) or [Delete Network Rule](#).
- Import - Lets you import an application rule or network rule. For more information, see [Import Content to Content Library](#).

## 2 Rule List Pane for 12.1 Version:

- Name - Name of the rule.
- Medium - Medium through which the rule is created.
- Last Updated - Displays the time when the rule is updated.
- Policies - Policies to which the rule is applied.


You can also sort on any column. If you mouse over a column header, a sort icon is displayed: .

Click the  icon to sort by the selected column.

## Rule List Pane for 12.1.1 Version:

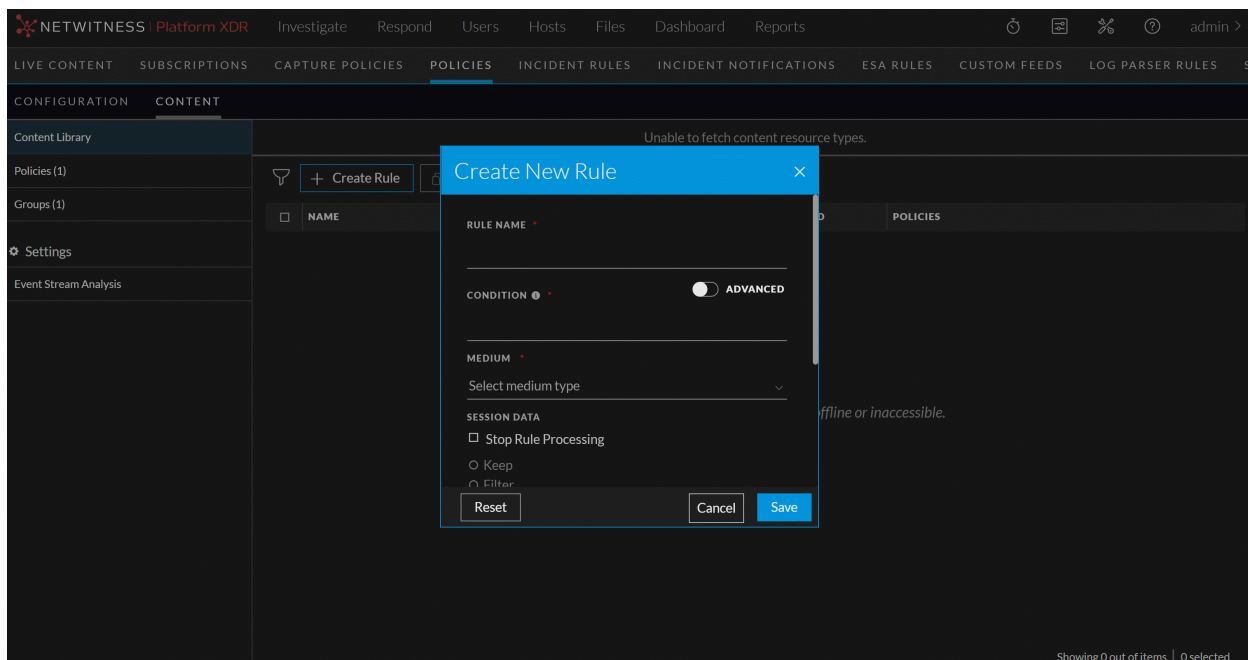
- Rule Name - Name of the rule.
- Rule Value - The rule value.
- Medium - Medium through which the rule is created.
- Last Updated - Displays the time when the rule is updated.
- Policies - Policies to which the rule is applied.

You can also sort on any column. If you mouse over a column header, a sort icon is displayed: .

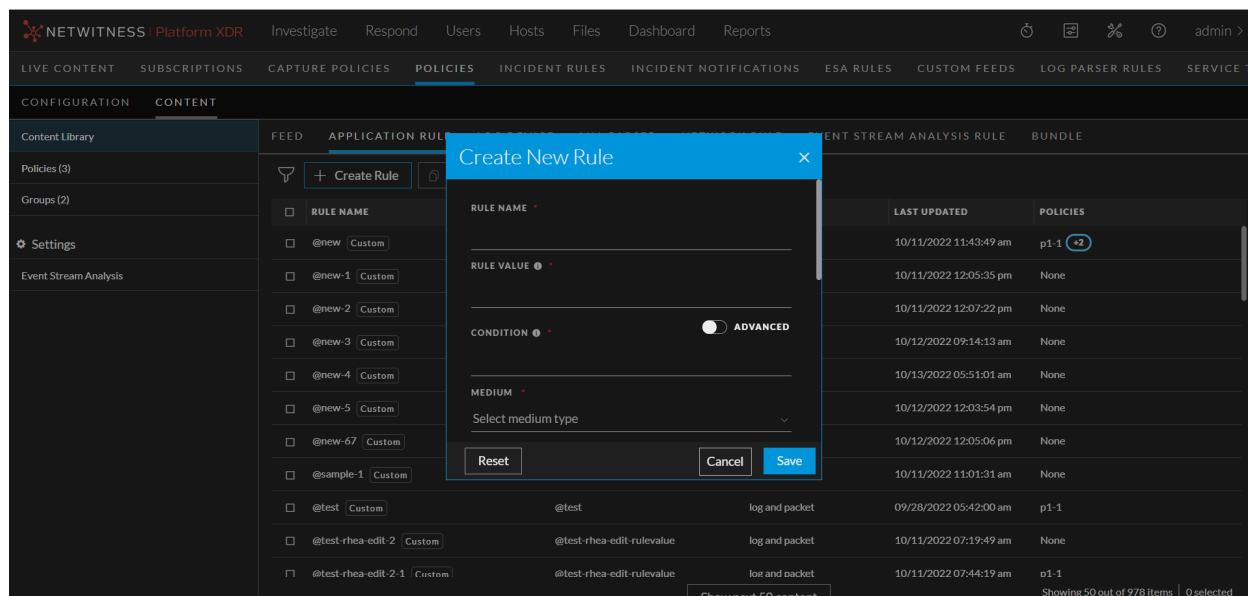
Click the  icon to sort by the selected column.

## Create New Rule dialog:

Below is an example of the Create new rule dialog for 12.1 version:



Below is an example of the Create new rule dialog for 12.1.1 version:



The table describes the information and options in the Create New Rule dialog:

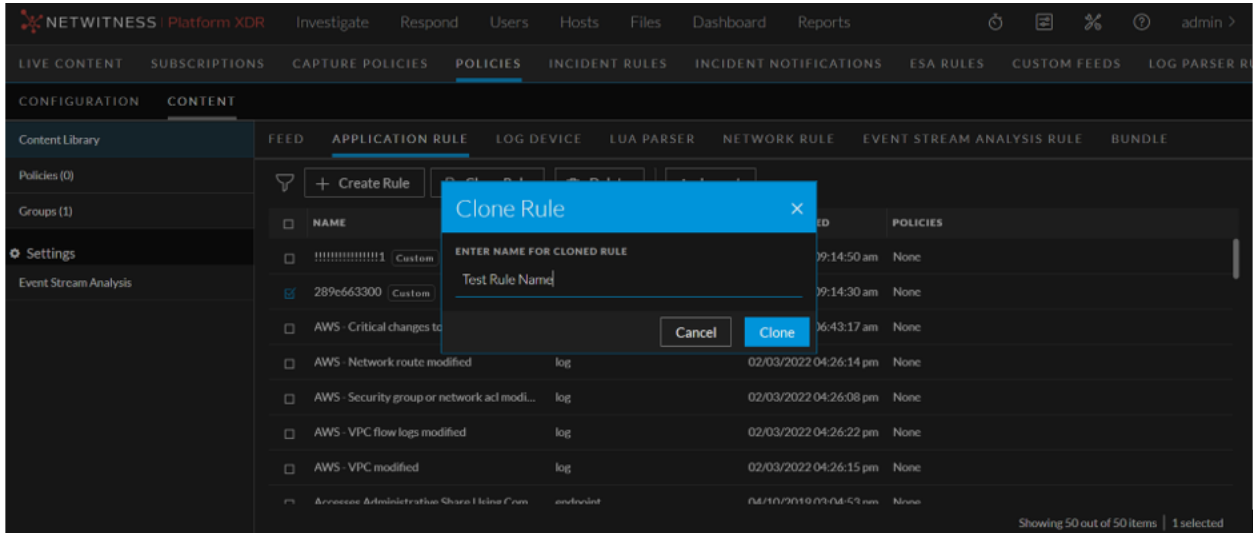
Field	Description
Rule Name	Name of the new rule. The name should be unique.
Rule Value	The rule value written to the alert meta. The rule value cannot be modified while cloning the rule. <b>Note:</b> This field is applicable only for 12.1.1 version.
Condition	Condition for the new rule. You can apply two types of conditions for the rule. <b>Normal mode:</b> It gives suggestions for supported metas (ip, host and so on) and operators (“=”, “Not Equal To”, “Contains”, “Exists” and so on). The entered condition will be enclosed in a ‘Pill’. When you enter multiple conditions, the conditions are automatically joined by an ‘AND’ operator. On clicking the ‘AND’ operator, you can toggle between ‘AND’ and ‘OR’ operators. <b>Advanced:</b> You can customize the conditions as a free form text.
Medium	Medium through which the rule is created. For a network rule, the value of medium is selected as Packet as default and the user cannot edit it.
Description	The description of the new rule.
Session Data	Session data for the new rule. Indicates if the rule processing should stop, keep, filter or truncate when the session data is running.
Session Options	Session options for the new rule. Indicates if the session options should be alert, forward or transient.
Alert On	Conditions for which the alert should be turned on.

**Save** Saves the settings and closes the Create New Rule dialog.

**Cancel** Cancels the operations.

**Clone Rule dialog:**

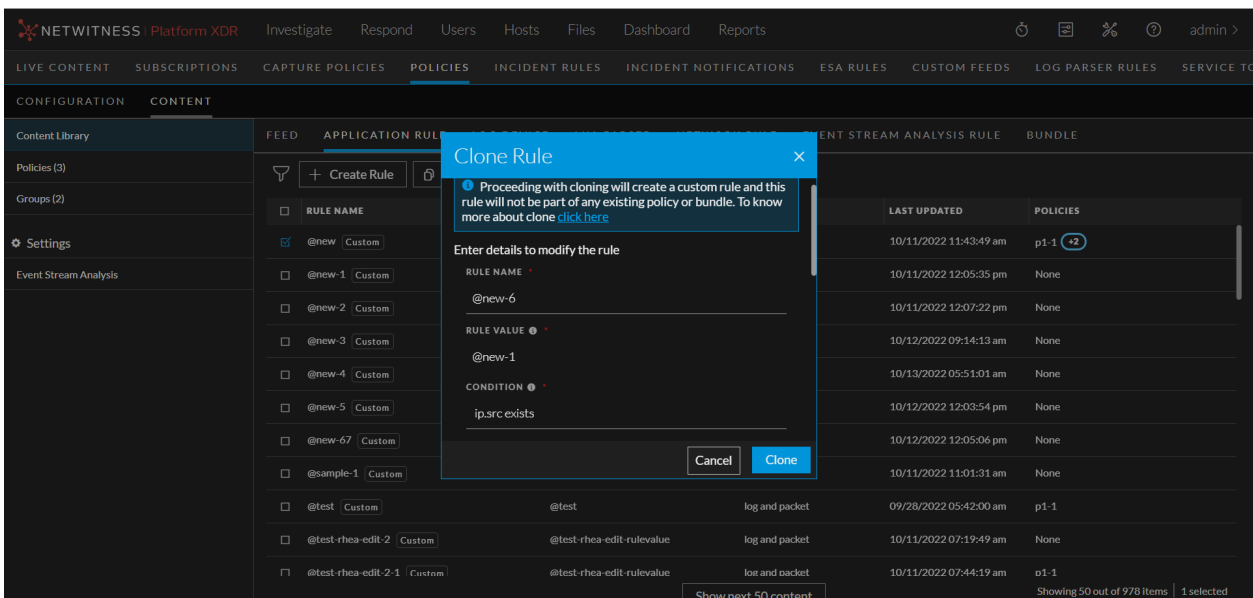
Below is an example of the Clone rule dialog for 12.1 version.



The table describes the information and options in the Clone Rule dialog for 12.1 version:

Field	Description
Enter Name for Cloned Rule	Name of the cloned rule. The name should be unique.
Clone	Clones the rule and closes the Cone Rule dialog.
Cancel	Cancels the operation.

Below is an example of the Clone rule dialog for 12.1.1 version.



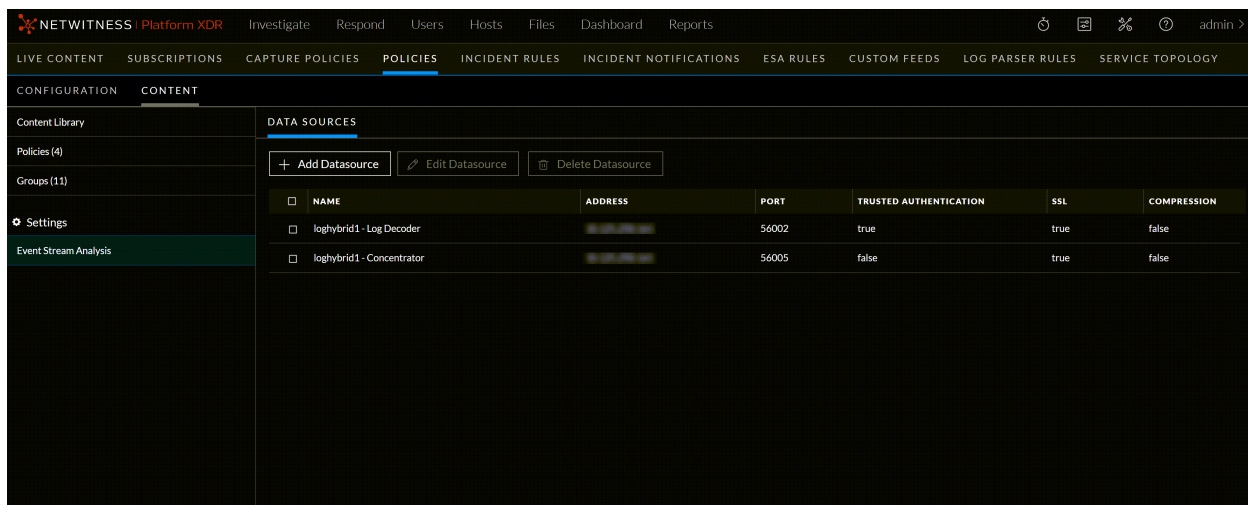
The table describes the information and options in the Clone Rule dialog for 12.1.1 version:

Field	Description
Rule Name	Name of the cloned rule. The name should be unique.
Rule Value	The rule value written to the alert meta. The rule value cannot be modified while cloning the rule.
Condition	<p>Condition for the new rule. You can apply two types of conditions for the rule.</p> <p><b>Normal mode:</b></p> <p>It gives suggestions for supported metas (ip, host and so on) and operators (“=”, “Not Equal To”, “Contains”, “Exists” and so on).</p> <p>The entered condition will be enclosed in a ‘Pill’. When you enter multiple conditions, the conditions are automatically joined by an ‘AND’ operator. On clicking the ‘AND’ operator, you can toggle between ‘AND’ and ‘OR’ operators.</p> <p><b>Advanced:</b></p> <p>You can customize the conditions as a free form text.</p>
Medium	Medium through which the rule is created. For a network rule, the value of medium is selected as <b>Packet</b> as default and you cannot edit it.
Description	The description of the new rule.
Session Data	Session data for the new rule. Indicates if the rule processing should stop, keep, filter or truncate when the session data is running.
Session Options	Session options for the new rule. Indicates if the session options should be alert, forward or transient.
Alert On	Conditions for which the alert should be turned on.
Clone	Clones the rule and closes the Cone Rule dialog.
Cancel	Cancels the operation.

## Data Sources Tab

Below is an example of the **Content > Settings > Event Stream Analysis > Data Sources** tab:





The following table describes the Data Sources tab.

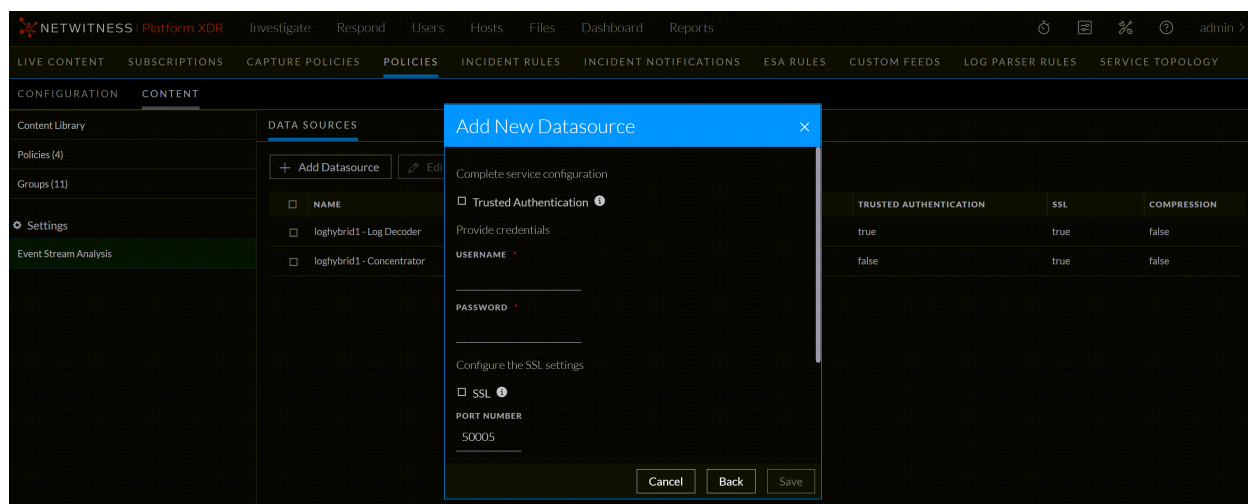
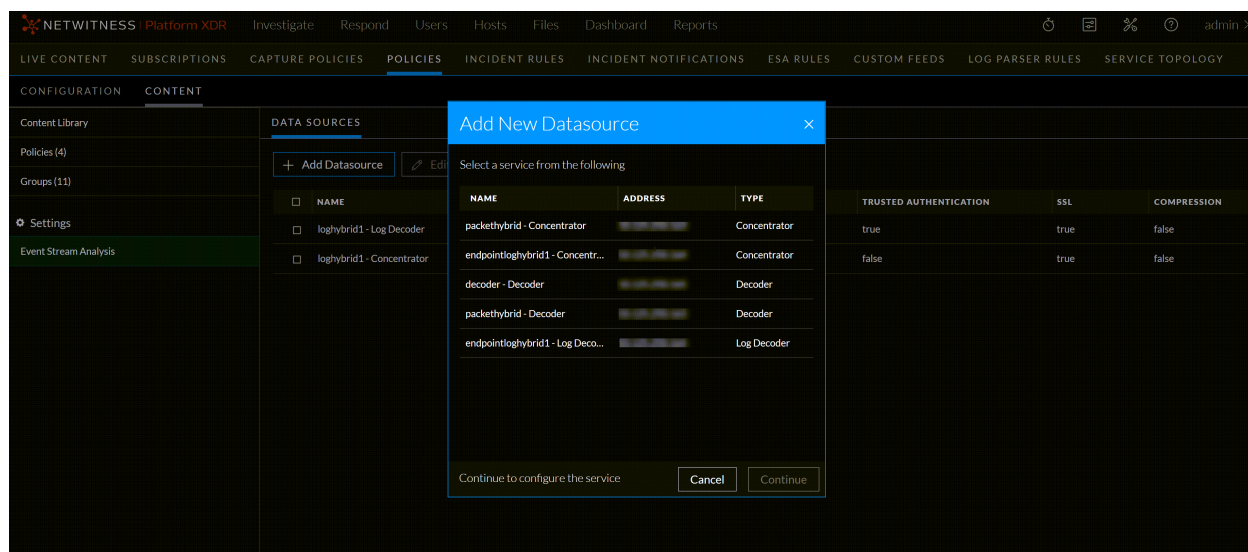
### 1 Toolbar

- Add Datasource- Lets you to add a new Datasource. For more information, see [Add an ESA Datasource](#).
- Edit - Datasource - Lets you edit the Datasource. For more information, see [Edit an ESA Datasource](#).
- Delete Datasource - Deletes the selected Datasource.

### 2 Data Sources List Pane

- Name - Shows the name of the data sources used by the selected ESA service. Data sources can be Concentrators or Decoders.
- Address - IP address of the datasource where the ESA service is installed.
- Port - Shows the port number used for authentication.
- Trusted Authentication - Indicates that it uses Trusted Authentication for communication with ESA Service.
- SSL - Indicates that it uses SSL for Authentication.
- Compression - Enables you to adjust the Compression Level on different datasources for ESA.

Below is an example of the **Add New Datasource** dialog:



The table describes the information and options in the **Add New Datasource** dialog.

Field	Description
Trusted Authentication	This option will enable the use of SSL by default for authentication.
Username	The username used to sign in to your account for authenticating the datasource.
Password	The password for authenticating the datasource.
SSL	This will enable the use of SSL for authentication.
Port Number	This will enable the use of the port number for authentication.
Compression	This option enables you to adjust the Compression Level on different datasources for ESA.
Compression Level	Enables you to set different compression level. Compression Level: <b>0</b> , <b>1</b> , and <b>9</b> . For more information, see <a href="#">Add an ESA Datasource</a> .

Field	Description
Test Configuration	Validates the provided configuration.
Save	Saves the settings and closes the Add New Datasource dialog.
Cancel	Cancels the operations.

## Deployments Tab

Below is an example of the **Content > Policies > select a policy > Event Stream Analysis Rule > Deployments** tab:

The screenshot shows the NetWitness Platform XDR interface. The breadcrumb trail is **Content Policy**. The main content area displays the **DEPLOYMENTS** tab for a policy named "Content Policy". The policy details are: DESCRIPTION: -, GROUPS: group1, POLICY STATUS: Unpublished, LAST UPDATED: 08/16/2022 09:49:04, CREATED ON: 08/10/2022 21:35:20, CREATED BY: admin. Below the details are buttons for **Publish Policy**, **Edit Policy**, **Merge Policy**, **Delete Policy**, and **Force Publish**. The **DEPLOYMENTS** section includes a toolbar with **Create Deployment**, **Remove Deployment**, **Deploy**, and **Stop Deployment**. A table lists three deployments:

NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	LAST UPDATED
Deployment1	esaprimary - ESA Correlation	loghybrid - Concentrator	Deployed	08/16/2022 09:50:02
Deployment2	esaprimary - ESA Correlation	loghybrid - Concentr... +1	New ▲	08/16/2022 09:50:36
Deployment3	esaprimary - ESA Correlation	loghybrid - Concentr... +2	Stopped	08/16/2022 09:51:04

Showing 3 out of 3 items | 0 selected

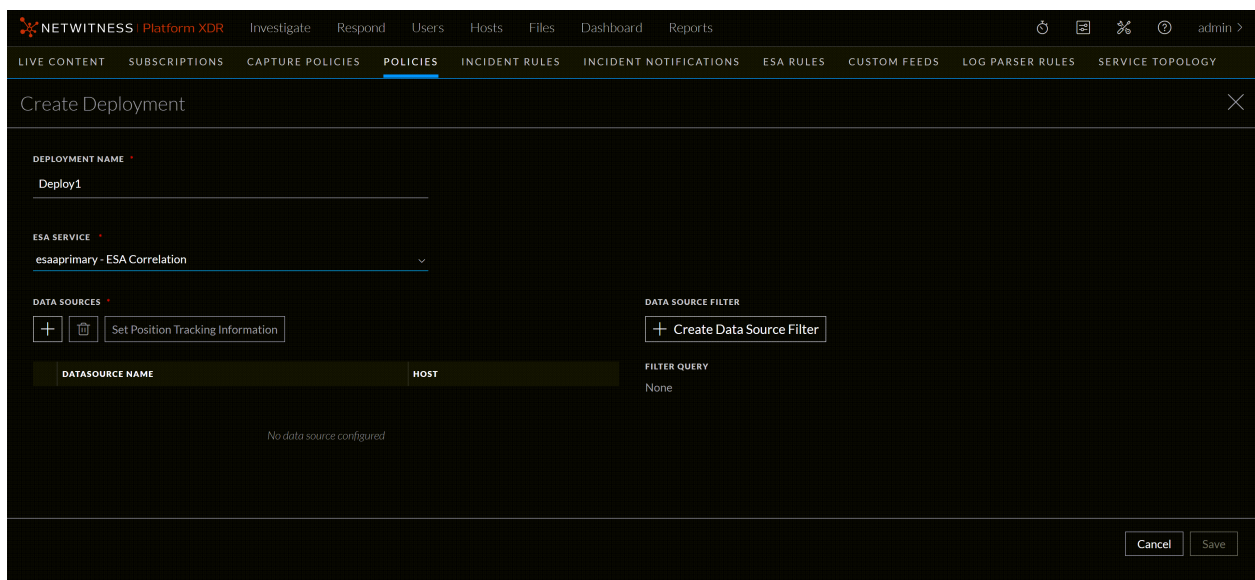
The following table describes the Deployments tab.

- 1 **Toolbar**
  - **Create Deployment** - Lets you to Add a new Deployment. For more information, see [Create a Deployment](#).
  - **Remove Deployment** - Lets you to remove the Deployment. For more information, see [Remove a Deployment](#).
  - **Deploy** - Lets you to deploy the Deployment.
  - **Stop Deployment** - Lets you to stop the selected Deployment.



- 2 Deployment List Pane
- Name - Name of the content.
  - ESA Service - Displays the ESA service selected.
  - Data Source - Displays the Datasource added for ESA deployment.
  - Deployment Status - Status of the deployment. The values are: Deploying, Deployed, New, Stopping, Stopped, and Failed.
  - Last Updated - Displays the time when the deployment is updated.

**Create Deployment dialog:**

Below is an example of the Create Deployment dialog:

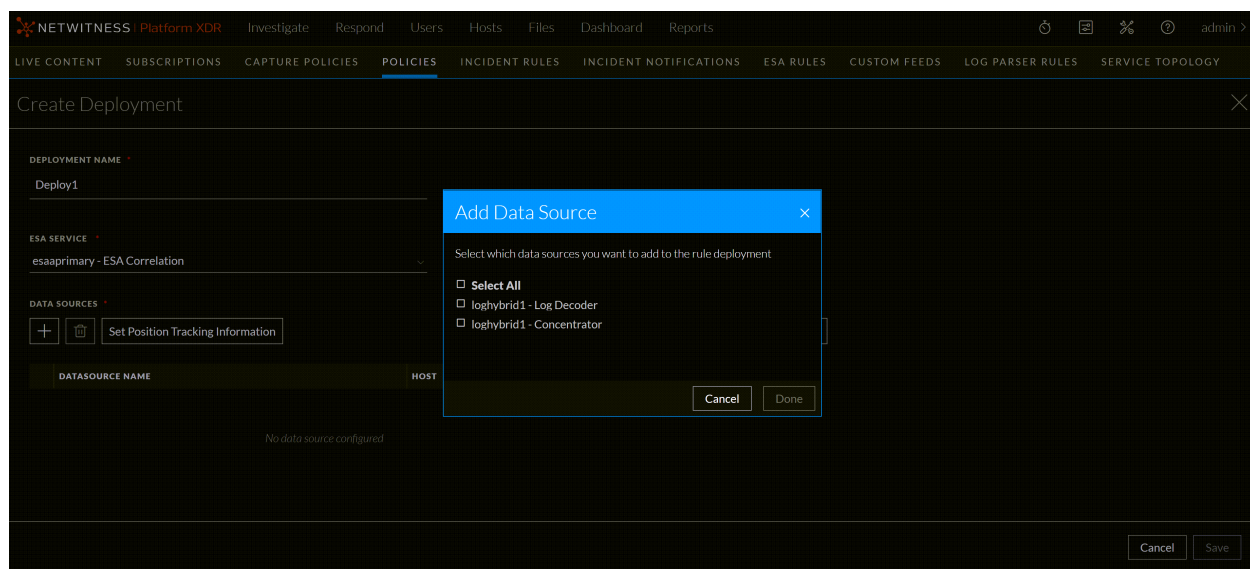


The table describes the information and options in the **Create Deployment** dialog.

Field	Description
Deployment Name	Name of the deployment. The name must be unique.
ESA Service	Displays the list of ESA services from the drop-down list. <ul style="list-style-type: none"> <li>• esaprimary – ESA Correlation</li> <li>• esasecondary – ESA Correlation</li> </ul>
	Adds a Datasource from the available list. At least one Datasource is required to set the position tracking information for ESA.
	Deletes the datasource that you are currently editing.

Field	Description
Set Position Tracking Information	Adds a position tracking information on different datasources for ESA. Position Tracking Information enables you to visualize the progress of the sessions that ESA has processed, and provides information on the session IDs and the time/date when the events were processed. For more information, see <a href="#">Appendix B: Position Tracking Information</a> .
Create Data Source Filter	Enables you to create the datasource filter to get the required results.
Save	Saves the settings and closes the Create Deployment dialog.
Cancel	Cancels the operations.

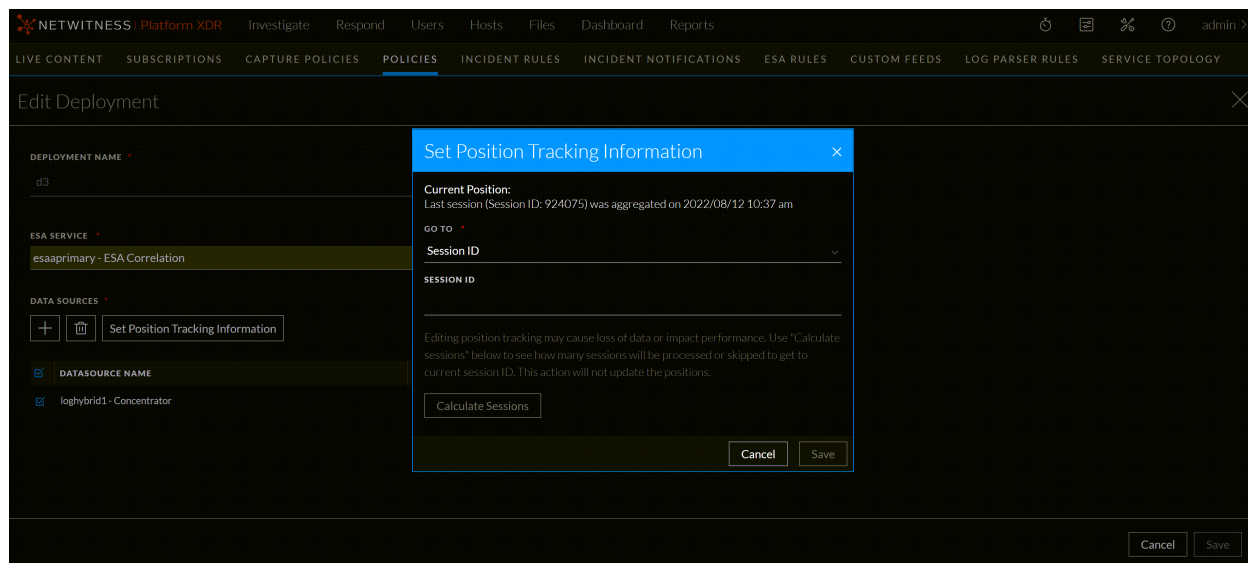
Below is an example of **Add Data Source Dialog**.



The table describes the information and options in the **Add Data Source** dialog.

Field	Description
Select Datasource / Select All	Allows you to select one or more datasources.
Done	Adds the datasource and closes the Add Data Source dialog.
Cancel	Cancels the operations.

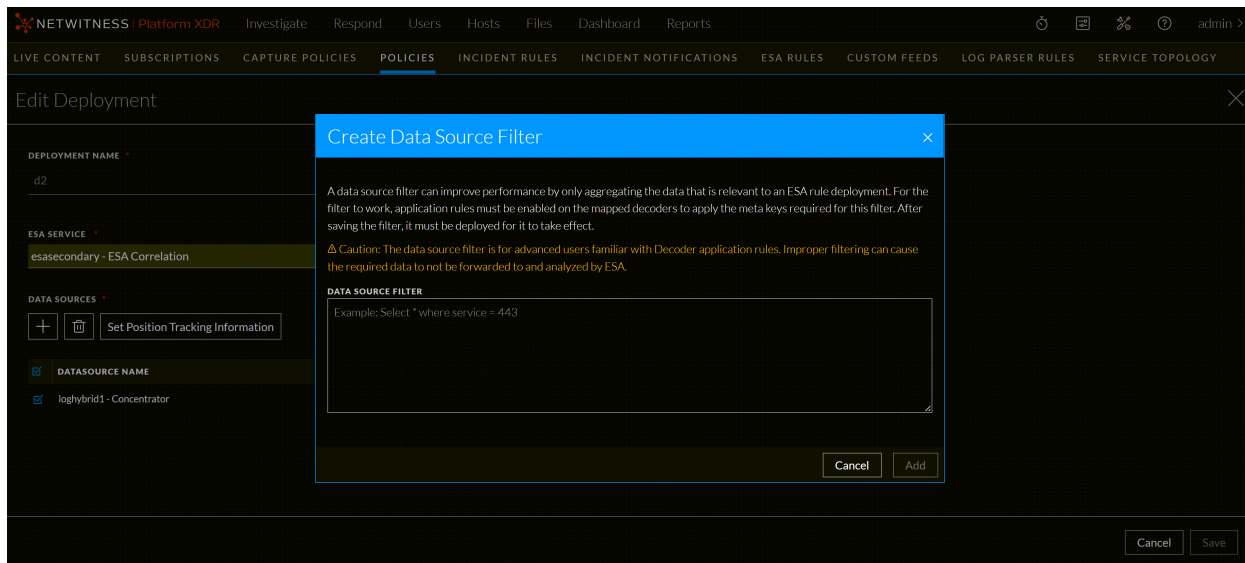
Below is an example of **Set Position Tracking Information** dialog.



The table describes the information and options in the **Set Position Tracking Information** dialog.

Field	Description
Go To	This option will enable the use of Session ID and data and time for ESA Correlation Service for the events.
Session ID	The ESA Correlation service starts processing the events from the session ID that you entered.
Date and Time	The ESA Correlation service starts processing the events from the date and time that you entered.
Calculate Sessions	This will calculate the number of sessions that will be processed with respect to the existing position of the data source.
Save	Saves the settings and closes the Set Position Tracking Information dialog.
Cancel	Cancels the operations.

Below is an example of **Create Data Source Filter** Dialog

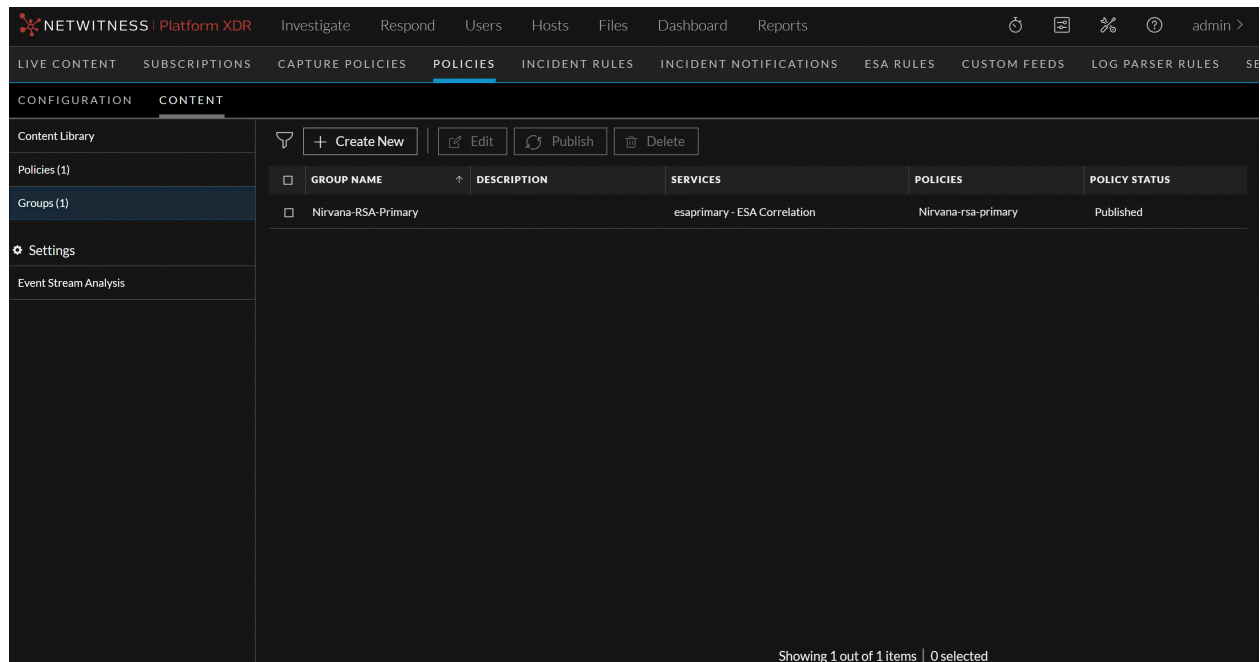


The table describes the information and options in the **Create Data Source Filter** dialog.

Field	Description
Data Source Filter	Enables you to enter the data source filter. For example, you can type <b>Select *where service = 443</b> to filter based on the query processed, it will filter out only HTTPS logs related sessions and will be forwarded to the ESA.
Add	Adds the configurations and closes the Create Data Source Filter dialog.
Cancel	Cancel the operations.

### Groups Tab

Below is an example of the **Content > Groups** tab:





The following table describes the Groups tab.

## 1 Toolbar

- Create New - Lets you create a new group. For more information, see [Create a group](#).
- Edit - Lets you edit the group. For more information, see [Managing Groups](#).
- Publish - Publishes selected groups.
- Delete - Deletes the selected group.

## 2 Group List Pane

- Group Name - Name of the group.
- Description - Description of the group.
- Services - Displays the service to the which the group is applied.
- Policies - Displays the policy to which the group is applied.
- Policy Status - Status of the policy. The values are: Published, Unpublished, Failed, N/A.

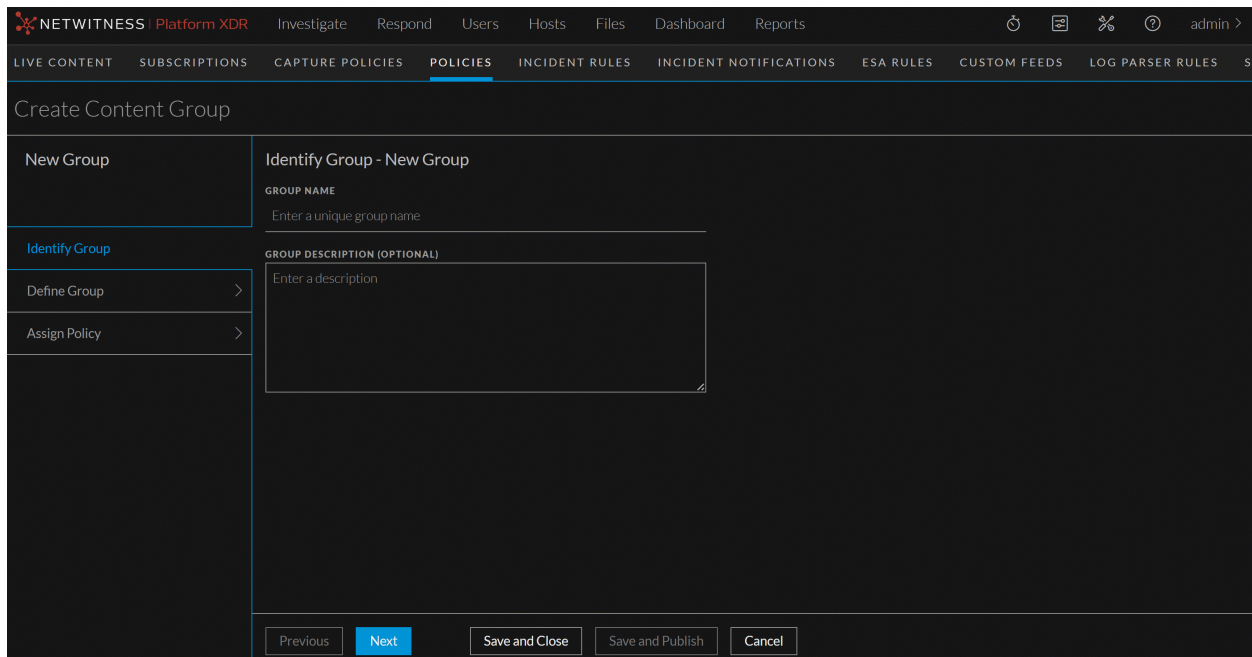
You can also sort on any column. If you mouse over a column header, a sort icon is displayed: . Click  to sort by the selected column.

## 3 Groups Details Panel

Displays the properties of the selected group.

Below is an example of the Create group dialog:

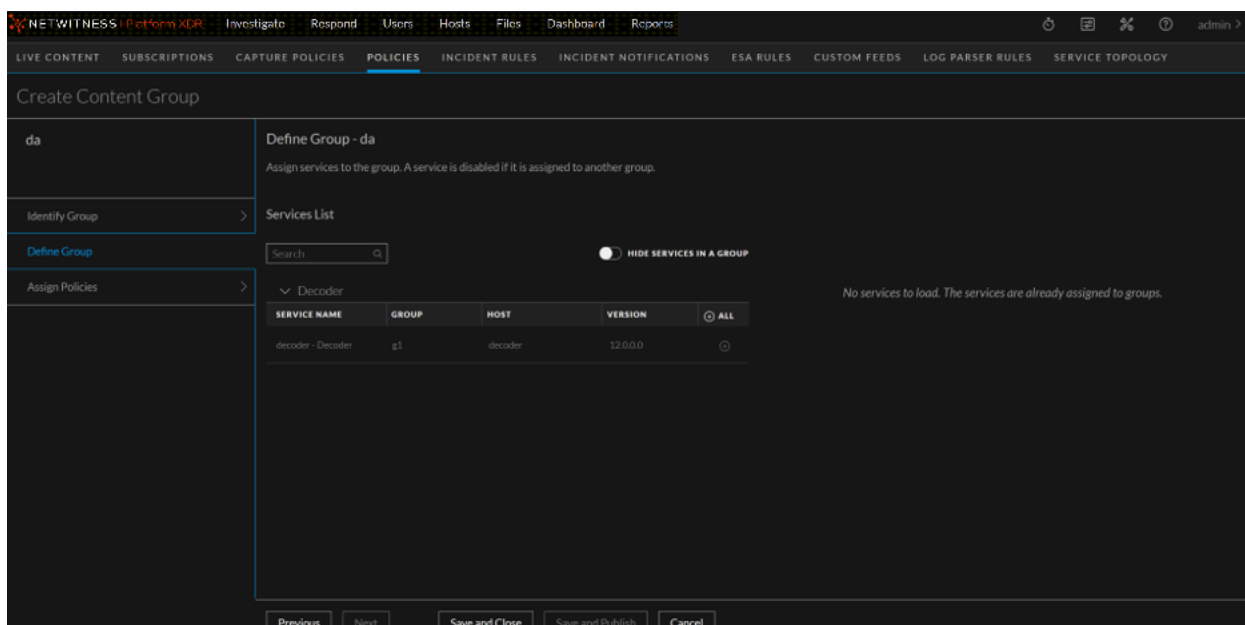




The table describes the information and options in the Create Group dialog:

Field	Description
Group Name	Name of the group. The name should be unique.
Group Description (Optional)	Description of the group. Description should not exceed 8000 characters.
Save and Close	Saves the settings and closes the Create Group dialog.

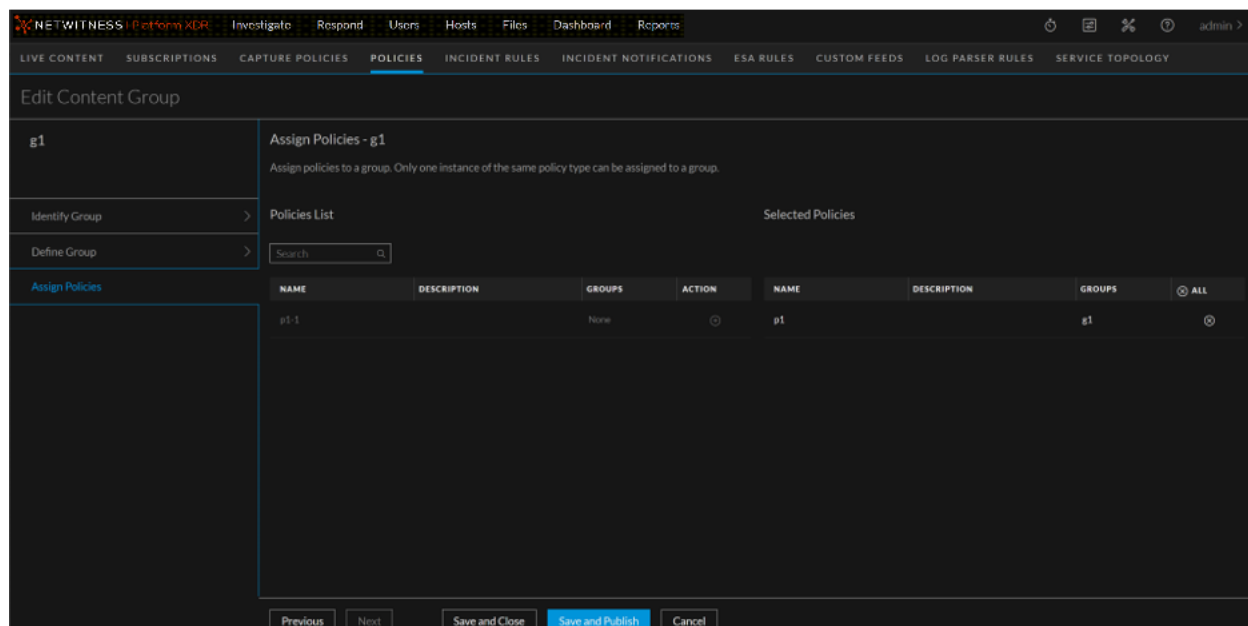
Below is an example of the define group dialog:



The table describes the information and options in the Define Group dialog:

Field	Description
Services List	<p>Displays the list of services.</p> <p>The following describes services list:</p> <p>Service name – Name of the service.</p> <ul style="list-style-type: none"> <li>• Group - Name of the group.</li> <li>• Host - Host name of the service.</li> <li>• Version - Service version.</li> <li>• All - Lets you to add services to the group. You can either click <b>⊕ ALL</b> to add all services or click <b>⊕</b> to add specific service.</li> </ul>
Hide Services in a Group	Displays the services that is not assigned to any group. By default, this option is disabled.
Selected Services	Displays the list of selected services for the group.
Save and Close	Saves the setting and closed the create group dialog.
Save and Publish	<p>Saves and publishes the created group.</p> <div style="border: 1px solid green; padding: 5px;"> <p><b>Note:</b> This option is disabled if you have not:</p> <ul style="list-style-type: none"> <li>- Assigned services.</li> <li>- Assigned policies.</li> </ul> </div>

Below is an example of Assign policy dialog:



The following table describes assign policy dialog:

Field	Description
-------	-------------

Policies List	<p>Displays the list of policies associated with the group.</p> <p>The following describes policies list:</p> <ul style="list-style-type: none"> <li>• Name - Name of the policy.</li> <li>• Description - Description of the policy.</li> <li>• Groups - Groups associated with the policy.</li> <li>• Action - Click to add policies to the group.</li> </ul>
Selected Policies	Displays the list of selected policies for the group.
Save and Close	Saves the setting and closed the create group dialog.
Save and Publish	Saves and publishes the created group.

**Note:** This option is disabled if you have not:

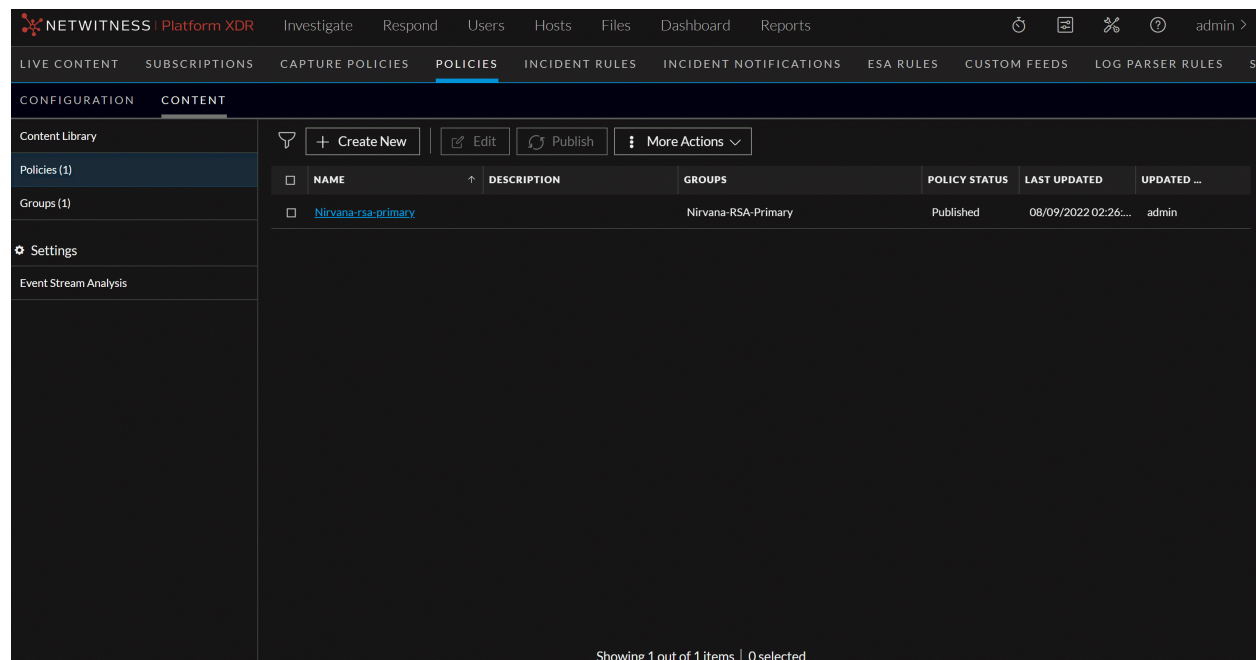
- Assigned services.
- Assigned policies.

## Policies Tab

**IMPORTANT:** The customers should note that, while publishing the first policy to a service, all previous content except custom feeds, will be deleted. Ensure that all custom content are migrated to Content Library before publishing the first policy.

The  (CONFIGURE) > Policies view contains two tabs: **Configuration** and **Content**.


Below is an example of the **Content > Policies** tab:



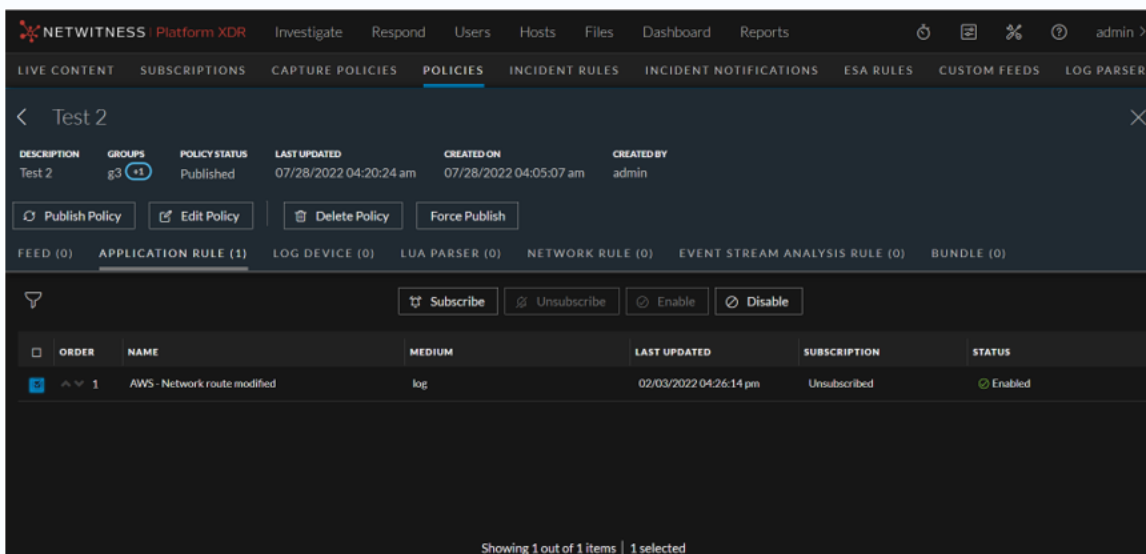
1 Toolbar:

- Create New - Lets you create a new policy. For more information, see Create a policy.
- Edit - Lets you edit the policy. For more information, see Edit a Policy.
- Publish - Publishes selected policy or policies.
- More Actions:
  - Assign to Group --Lets you assign policy to a group.
  - Clone - Lets you clone a policy.
  - Delete - Deletes the selected group or groups permanently.
  - Force Publish - Lets you republish all the content irrespective of the policy status. This option allows you to re-push all content or configurations to all services in the group. Some of the scenarios where you might want to force publish the policy are:
    - There was a service that was down or did not successfully receive content when it was first pushed out.
    - Some content may have been modified or removed locally on a service (outside of CCM control) and you want to re-apply the content from the policy.

2 Policy List Pane:

- Name - Name of the policy.
- Description - Description of the policy.
- Groups - Lists the group to which this policy is applied.
- Policy Status - Status of the policy. The values are: Published, Unpublished, Failed, N/A.
- Last Updated - Displays the time when the policy is updated.
- Updated By - The user who updated the policy. You can also sort on any column. If you mouse over a column header, a sort icon is displayed: . Click the  icon to sort by the selected column.

### 3 Policy Details Panel:



Displays the Displays the properties of the selected policy.

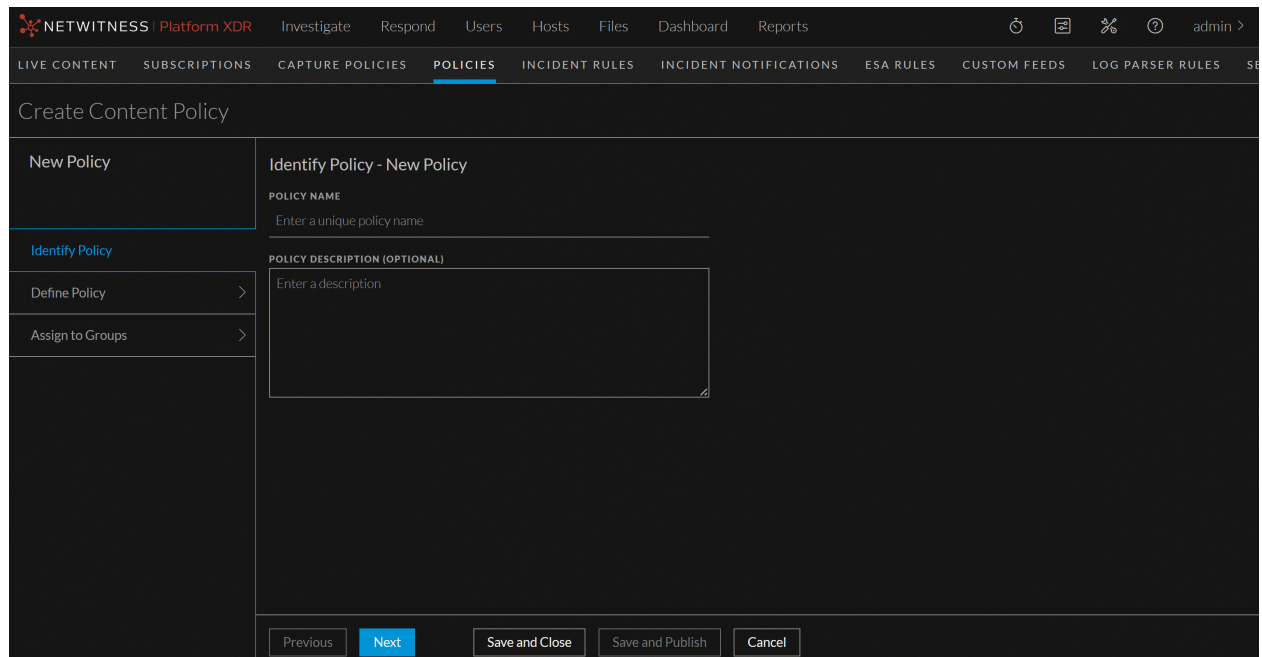
Toolbar:

- Publish Policy - Lets you publish all the unpublished and/or failed content. For more information, see Create a Policy.
- Edit Policy - Lets you edit the policy. For more information, see Edit a Policy.
- Delete Policy - Deletes the selected policy or policies permanently.
- Force Publish - Lets you republish all the content irrespective of the policy status.

Policy Details Pane:

- Order - Order of the content.
- Name - Name of the content.
- Medium - Meta data source medium.
- Last Updated - Displays the time when the content is last updated.
- Subscription - Indicates if the content is subscribed or unsubscribed.
- Status - The status of resource.
- Subscribe - Lets you subscribe for the content if it is unsubscribed.
- Unsubscribe - Lets you unsubscribe for the content if it is subscribed.
- Enable - Lets you enable the content for the policy.
- Disable - Lets you disable the content from the policy.

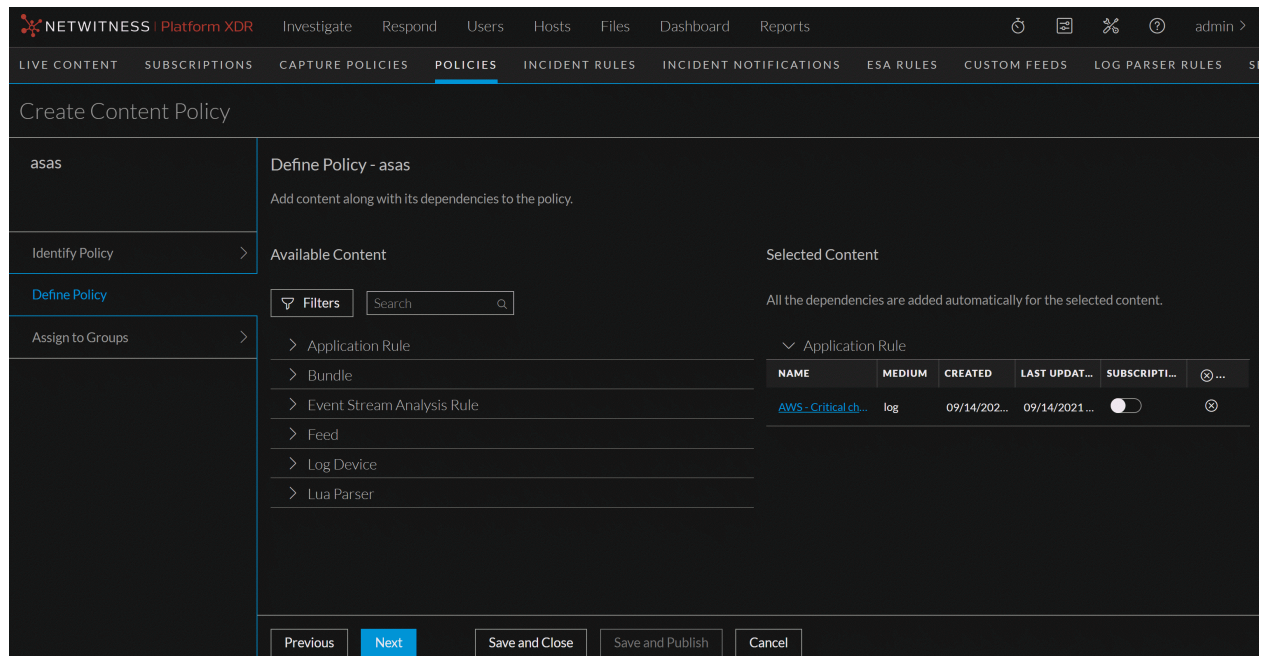
Below is an example of the Create Content Policy dialog.



The table describes the information and options in the Create Policy dialog:

Field	Description
Policy Name	Name of the policy. The name should be unique.
Policy Description (Optional)	Description of the policy. Description should not exceed 8000 characters.

### Define Policy Settings:



**Field****Description**

Available Content

Displays the available content resources in your deployment. Click expand the resource type.

The screenshot shows the 'Available Content' section in the NetWitness Platform XDR interface. The interface includes a navigation bar with 'POLICIES' selected, a 'Create Content Policy' header, and a 'Define Policy - asas' section. The 'Available Content' table lists various resources with columns for Name, Medium, Created, Last Updated, and Action. The 'Selected Content' section shows a single resource, 'AWS - Critical ch...', with a toggle switch and an action icon.

NAME	MEDIUM	CREATED	LAST UPDATED	ACTI...
AWS - Network ro...	log	02/03/2022 0...	02/03/2022 0...	⊕
AWS - Security gr...	log	02/03/2022 0...	02/03/2022 0...	⊕
AWS - VPC flow lo...	log	02/03/2022 0...	02/03/2022 0...	⊕
AWS - VPC modified	log	02/03/2022 0...	02/03/2022 0...	⊕
Accesses Administ...	endpoint	04/10/2019 0...	04/10/2019 0...	⊕
Activates BITS Job	endpoint	04/10/2019 0...	04/10/2019 0...	⊕

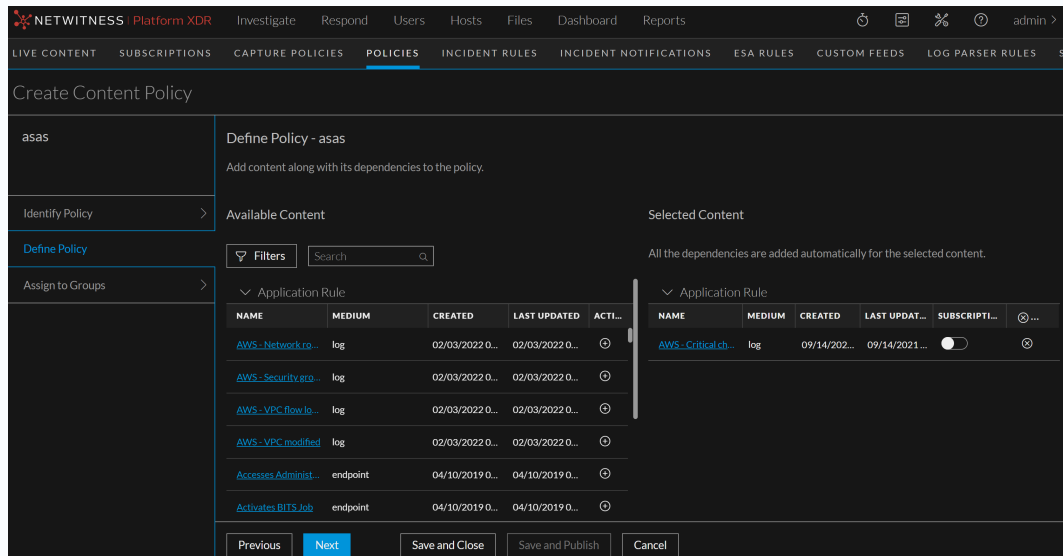
The following describes resource type:

- Name - Name of the resource.
- Medium - Meta data source medium. Available values for medium are as follows:
  - **Endpoint:** applied to content that uses meta derived from endpoint agent and endpoint server data
  - **Log:** applied to content that uses meta derived from log data
  - **Packet:** applied to content that uses meta derived from network packets
  - **Log and packet:** applied to content that correlates meta derived across log and packet data
- Created - Displays the time when the resource is created
- Last Updated - Displays the time when the resource is updated last.
- Action- Click + to add the resource and its dependencies to your deployment.

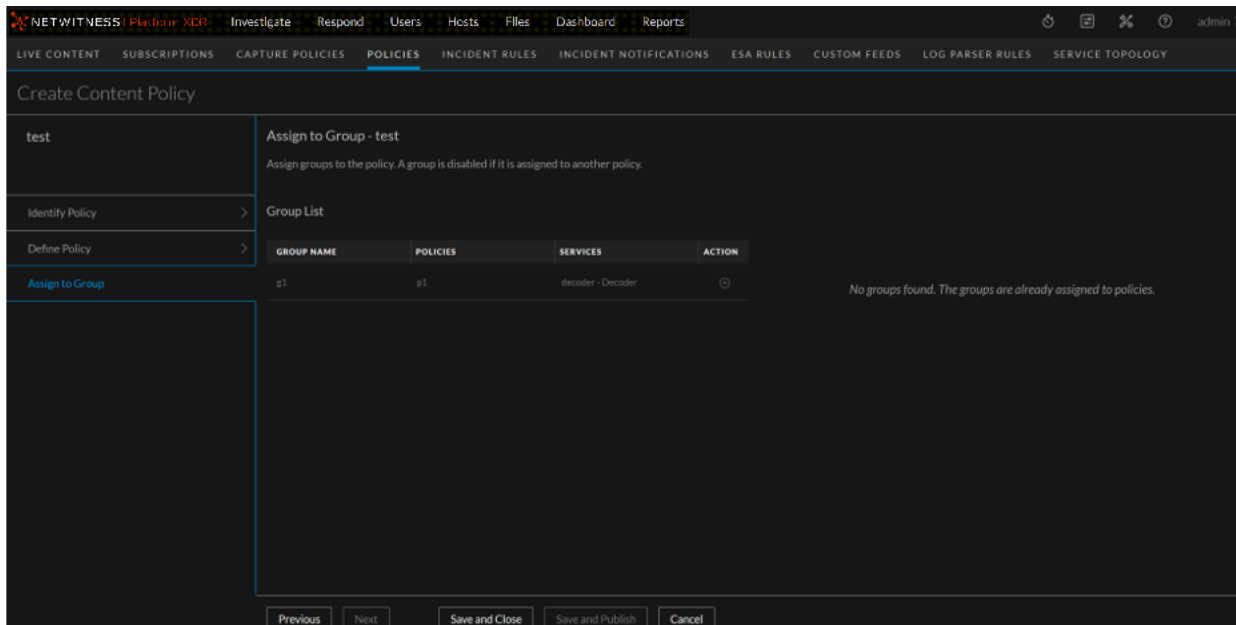
**Selected Content**

Lists the selected resource.


Additionally, you can subscribe the content. Once the content is subscribed, the content resources are updated automatically in case of any changes.



**Assign to Group:**





<b>Group List</b>	Displays the list of groups associated with the policy. A group is disabled if it is already assigned to another policy. <ul style="list-style-type: none"> <li>• Group Name</li> <li>• Policies</li> <li>• Services</li> <li>• Action</li> </ul>
<b>Selected Group</b>	Lists the selected groups. Click  to add groups.
<b>Save and Close</b>	Saves the settings and closes the Create Policy dialog.
<b>Save and Publish</b>	Saves and publishes the created policy. <div style="border: 1px solid green; padding: 5px; margin-top: 5px;"> <p><b>Note:</b> This option is disabled if:</p> <ul style="list-style-type: none"> <li>- Policy settings are not customized.</li> <li>- Policy is not assigned to groups.</li> </ul> </div>

## Appendix A: Endpoint Risk Scoring Rules

Endpoint risk scoring requires the following content:

- "accesses administrative share using command shell"
- "activates bits job"
- "adds files to bits download job"
- "adds firewall rule"
- "allocates remote memory"
- "antivirus disabled"
- "archiving software reads multiple documents"
- "autorun debian package mismatch"
- "autorun file path not part of debian package"
- "autorun file path not part of rpm"
- "autorun key contains non-printable characters"
- "autorun"
- "autorun rpm mismatch"
- "autorun unsigned active setup"
- "autorun unsigned appinit\_dlls"

- "autorun unsigned bho"
- "autorun unsigned bootexecute registry startup method"
- "autorun unsigned explorer registry startup method"
- "autorun unsigned hidden"
- "autorun unsigned hidden only executable in directory"
- "autorun unsigned ie toolbar"
- "autorun unsigned in appdata local directory"
- "autorun unsigned in appdata roaming directory"
- "autorun unsigned in program data directory"
- "autorun unsigned in temp directory"
- "autorun unsigned logon type registry startup method"
- "autorun unsigned lsa provider"
- "autorun unsigned servicedll"
- "autorun unsigned winlogon helper dll"
- "autorun unsigned winsock lsp"
- "bad certificate warning disabled"
- "blacklisted file"
- "browser runs command prompt"
- "browser runs mshta"
- "browser runs powershell"
- "builds script incrementally"
- "clears application event log"
- "clears event logs using powershell"
- "clears security event log"
- "clears setup event log"
- "clears system event log"
- "combines binaries using command prompt"
- "command line usage of archiving software"
- "command line writes script files"
- "command prompt obfuscation"

- "command prompt obfuscation using value extraction"
- "command shell runs rundll32"
- "completes bits download job"
- "configures image hijacking"
- "configures port redirection"
- "copies binary over administrative share"
- "created in last month"
- "creates browser extension"
- "creates domain user account"
- "creates executable in startup directory"
- "creates local driver service"
- "creates local service"
- "creates local task"
- "creates local user account"
- "creates password-protected archive"
- "creates recursive archive"
- "creates remote process using wmi command-line tool"
- "creates remote service"
- "creates remote task"
- "creates run key"
- "creates shadow volume for logical drive"
- "creates suspicious service running command prompt"
- "debian package hash mismatch in important system directory"
- "debian package hash mismatch"
- "deletes backup catalog"
- "deletes firewall rule"
- "deletes shadow volume copies"
- "deletes shadow volume copies using powershell"
- "deletes usn change journal"
- "disables event logging service"

- "disables firewall"
- "disables safe mode"
- "disables security service"
- "disables startup repair"
- "disables uac"
- "disables uac remote restrictions"
- "disables windows audit policy"
- "disables windows defender using powershell"
- "downloads binary using certutil"
- "drops credential dumping tools"
- "dumps dns cache"
- "dyld inserted"
- "enables cleartext credential storage"
- "enables login bypass"
- "enables rdp from command-line"
- "enables safe mode"
- "enumerates arp table"
- "enumerates available systems on network"
- "enumerates domain account policy"
- "enumerates domain administrators"
- "enumerates domain computers"
- "enumerates domain controllers"
- "enumerates domain groups"
- "enumerates domain users"
- "enumerates enterprise administrators"
- "enumerates exchange domain servers"
- "enumerates exchange servers"
- "enumerates ip configuration"
- "enumerates local account policy"
- "enumerates local administrators"

- "enumerates local administrators on domain controller"
- "enumerates local groups"
- "enumerates local services"
- "enumerates local users"
- "enumerates logical disk"
- "enumerates mapped resources"
- "enumerates network connections"
- "enumerates primary domain controller"
- "enumerates processes on local system"
- "enumerates processes on remote system"
- "enumerates remote netbios name table"
- "enumerates remote resources"
- "enumerates route table"
- "enumerates services hosted in processes"
- "enumerates system info"
- "enumerates trusted domains"
- "evades scanning within windows defender"
- "evasive powershell used over network"
- "event viewer executes uncommon binary"
- "execute dll through rundll32"
- "exports sensitive registry hive"
- "extracts password-protected archive"
- "file encrypted"
- "file hidden"
- "file path not part of debian package in important system directory"
- "file path not part of debian package"
- "file path not part of rpm in important system directory"
- "file path not part of rpm"
- "file vault disabled"
- "floating module and hooking"

- "floating module in browser process"
- "floating module in os process"
- "floating module"
- "gatekeeper disabled"
- "gets current user as system"
- "gets current username and group information"
- "gets current username"
- "gets hostname"
- "gets remote time"
- "gina replacement"
- "graylisted file"
- "hidden and hooking"
- "hidden in appdata"
- "hidden plist and autorun"
- "hidden running as root"
- "hooks audio output function"
- "hooks authentication function"
- "hooks crypto function"
- "hooks dnsquery function"
- "hooks gui function"
- "hooks network http function"
- "hooks network io function"
- "hooks ntldr function"
- "hooks registry access function"
- "hooks registry enumeration function"
- "http daemon runs command prompt"
- "http daemon runs powershell"
- "http daemon runs reconnaissance tool"
- "http daemon writes executable"
- "ie dep disabled"

- "ie enhanced security disabled"
- "in appdata directory"
- "in hidden directory"
- "in recycle bin directory"
- "in root of appdata local directory"
- "in root of appdata roaming directory"
- "in root of logical drive"
- "in root of program directory"
- "in root of users directory"
- "installs root certificate"
- "in system volume information directory"
- "in temporary directory"
- "in uncommon directory"
- "invalid signature"
- "next signature validation disabled"
- "lateral movement with credentials using net utility"
- "ld preload"
- "library preferences directory"
- "lists anti-spyware products"
- "lists antivirus products"
- "lists firewall products"
- "login bypass configured"
- "lua disabled"
- "mac firewall disabled"
- "malicious file by reputation service"
- "maps administrative share"
- "maps ipc\$ share"
- "misleading file extension"
- "modifies file associations"
- "modifies image file execution for persistence"

- "modifies registry using command-line registry tool"
- "modifies run key"
- "modifies shell-open-command file association"
- "modifies startup folder location"
- "modifies winlogon dll for persistence"
- "modifies winlogon registry settings"
- "mshta runs command prompt"
- "mshta runs powershell"
- "mshta runs scripting engine"
- "mshta writes executable"
- "network access"
- "no antivirus notification disabled"
- "no firewall notification disabled"
- "non-microsoft modifies bad certificate warning setting"
- "non-microsoft modifies firewall policy"
- "non-microsoft modifies internet zone setting"
- "non-microsoft modifies lua setting"
- "non-microsoft modifies registry editor setting"
- "non-microsoft modifies security center config"
- "non-microsoft modifies services imagepath"
- "non-microsoft modifies task manager setting"
- "non-microsoft modifies windows system policy"
- "non-microsoft modifies zone crossing warning setting"
- "no uac notification disabled"
- "no windows update notification disabled"
- "office application crashed"
- "office application injects remote process"
- "office application runs bits"
- "office application runs command prompt"
- "office application runs powershell"



- "office application runs scripted ftp"
- "office application runs scripting engine"
- "office application runs task scheduler"
- "office application runs wmi scripting engine"
- "office application writes executable"
- "opens browser process"
- "opens os process"
- "opens process"
- "opswat reported infected"
- "opswat reported suspicious"
- "os process runs command shell"
- "packed and autorun"
- "packed and network access"
- "packed"
- "performs scripted file transfer"
- "possible login bypass"
- "possible mimikatz activity"
- "possible rdp session hijacking"
- "possibly configures uac bypass"
- "possibly renamed net.exe detected"
- "potential abuse of odbconf"
- "potential outlook exploit"
- "powershell command using string manipulation"
- "powershell injects remote process"
- "powershell opens lsass process"
- "powershell runs command prompt"
- "powershell runs scripting engine"
- "process authorized in firewall"
- "process redirects to stdout or stderr"
- "process with matched yara rule"

- "process with opswat reported infected"
- "process with opswat reported suspicious"
- "psexesvc runs powershell"
- "psexesvc runs scripting engine"
- "psexesvc runs shell commands"
- "pubprn detection"
- "queries cached kerberos tickets"
- "queries processes on local system"
- "queries processes on remote system"
- "queries registry using command-line registry tool"
- "queries terminal sessions"
- "queries users logged on local system"
- "queries users logged on remote system"
- "record screen captures using psr tool"
- "registers always install elevated policy"
- "registers appcert dll"
- "registers appinit dll"
- "registers boot execute"
- "registers lsa authentication package"
- "registers lsa notification package"
- "registers lsa security package"
- "registers netsh helper dll"
- "registers port monitor dll"
- "registers shim database"
- "registers startup during safe mode boot"
- "registers time provider dll"
- "registry tools disabled"
- "regsvr32 creates windows task"
- "regsvr32 runs powershell"
- "regsvr32 runs rundll32"

- "regsvr32 writes executable"
- "remote directory traversal"
- "removes windows defender definitions"
- "rpm hash mismatch in important system directory"
- "rpm hash mismatch"
- "rpm ownership changed"
- "rpm permissions changed"
- "rundll32 creates windows task"
- "rundll32 runs powershell"
- "runkey persistence"
- "runs acl management tool"
- "runs active directory service query tool"
- "runs binary located in recycle bin directory"
- "runs binary located in root of logical drive"
- "runs binary located in root of program directory"
- "runs binary located in root of users directory"
- "runs binary located in system volume information directory"
- "runs blacklisted file"
- "runs certutil with decode arguments"
- "runs certutil with encode arguments"
- "runs certutil with hashfile arguments"
- "runs chained command shell"
- "runs chmod"
- "runs credential dumping tools"
- "runs curl"
- "runs ditto"
- "runs dns lookup tool for txt record"
- "runs dns lookup tool"
- "runs file attributes modification tool"
- "runs file transfer tool"

- "runs forfiles.exe"
- "runs graylisted file"
- "runs ifconfig"
- "runs kextload"
- "runs kextstat"
- "runs launchctl"
- "runs malicious file by reputation service"
- "runs mshta with http argument"
- "runs mshta with script argument"
- "runs msiexec with http argument"
- "runs netstat"
- "runs network configuration tool"
- "runs network connectivity tool"
- "runs one letter executable"
- "runs one letter script"
- "runs ping"
- "runs powershell bypassing execution policy"
- "runs powershell decoding base64 string"
- "runs powershell defining function"
- "runs powershell downloading content"
- "runs powershell invoke-mimikatz function"
- "runs powershell memory stream function"
- "runs powershell"
- "runs powershell shellexecute function"
- "runs powershell using encoded command"
- "runs powershell using environment variables"
- "runs powershell with hidden window"
- "runs powershell with http argument"
- "runs powershell with long arguments"
- "runs psexec on remote system and silently accepts user license"

- "runs psexec on remote system as system user"
- "runs ps"
- "runs registry tool"
- "runs regsvr32 com scriplets"
- "runs regsvr32 using one letter dll"
- "runs regsvr32 with http argument"
- "runs regsvr32 without arguments"
- "runs remote execution tool"
- "runs remote powershell command"
- "runs robocopy.exe"
- "runs rundll32 using one letter dll"
- "runs rundll32 with http argument"
- "runs rundll32 with javascript argument"
- "runs rundll32 without arguments"
- "runs scripting engine in batch mode using execution engine argument"
- "runs scripting engine"
- "runs service control tool"
- "runs shim database installer"
- "runs sh"
- "runs suspicious file by reputation service"
- "runs tar"
- "runs tasks management tool"
- "runs unzip"
- "runs waitfor.exe"
- "runs wmi command-line tool"
- "runs wmi scripting engine"
- "runs xcopy.exe"
- "safari fraud website warning disabled"
- "scripting addition in process"
- "scripting engine injects remote process"

- "scripting engine runs powershell"
- "scripting engine runs regsvr32"
- "scripting engine runs rundll32"
- "self signed"
- "services in programdata directory"
- "services runs command shell"
- "smartscreen filter disabled"
- "starts local service"
- "starts rdp service"
- "starts remote service"
- "stops diagtrack service"
- "stops error reporting service"
- "stops security service"
- "stops windows update service"
- "sudo no password prompt"
- "suspicious file by reputation service"
- "suspicious regsvr32.exe task"
- "system integrity protection disabled"
- "system restore disabled"
- "tampers with windows defender registry"
- "task manager disabled"
- "tasks in programdata directory"
- "terminates process"
- "transfers file using bits"
- "uac disabled"
- "unexpected csrss.exe parent"
- "unexpected explorer.exe destination location"
- "unexpected explorer.exe parent"
- "unexpected explorer.exe source location"
- "unexpected lsass.exe parent"

- "unexpected lsm.exe parent"
- "unexpected msdtc.exe parent"
- "unexpected os process destination location"
- "unexpected os process source location"
- "unexpected runtimebroker.exe parent"
- "unexpected services.exe parent"
- "unexpected smss.exe parent"
- "unexpected svchost arguments"
- "unexpected svchost.exe parent"
- "unexpected taskhostw.exe parent"
- "unexpected wininit.exe parent"
- "unexpected winlogon.exe parent"
- "unknown segment"
- "unsigned copies self"
- "unsigned creates remote thread and file hidden"
- "unsigned creates remote thread"
- "unsigned cron job"
- "unsigned deletes self"
- "unsigned kext"
- "unsigned library in suspicious daemon"
- "unsigned module in signed process"
- "unsigned reserved name"
- "unsigned runs python"
- "unsigned writes executable"
- "unsigned writes executable to appdata local directory"
- "unsigned writes executable to appdata roaming directory"
- "unsigned writes executable to library application support directory"
- "unsigned writes executable to library directory"
- "unsigned writes executable to library preferences directory"
- "unsigned writes executable to scripting additions directory"

- "unsigned writes executable to system directory"
- "unsigned writes executable to var directory"
- "unsigned writes executable to windows directory"
- "unsigned writes to autorun"
- "uses libnss"
- "uses libpcap"
- "uses mach injection"
- "uses mach override"
- "warning on post redirect disabled"
- "windows firewall disabled"
- "windows task runs powershell"
- "windows update disabled"
- "wmic remote node activity"
- "wmiprvse runs command shell"
- "wmiprvse runs powershell"
- "wmiprvse runs scripting engine"
- "writes blacklisted file"
- "writes executable to recycle bin directory"
- "writes executable to root of logical drive"
- "writes executable to root of program directory"
- "writes executable to root of users directory"
- "writes executable to system volume information directory"
- "writes graylisted file"
- "writes malicious file by reputation service"
- "writes suspicious file by reputation service"
- "yara rule matched"
- "executable in ads"
- "explorer public folder dll load"
- "powershell double base64"
- "outbound from windows directory"



- "outbound from unsigned temporary directory"
- "unsigned opens lsass"
- "outbound from unsigned appdata directory"
- "rdp launching loopback address"
- "autorun invalid signature windows directory"
- "command shell copy items"

## Appendix B: Position Tracking Information

The ESA Correlation service continuously streams data from the data sources like decoders (log and network), and concentrators. ESA retrieves events from the data sources, and applies rules to generate alerts to detect malicious activities. When you deploy a data source, ESA starts processing information from the latest available session, by default. Position Tracking Information enables you to visualize the progress of the sessions that ESA has processed, and provides information on the session IDs and the date and time when the events were processed.

Set Position Tracking Information enables you to:

- Visualize the number of sessions that a particular ESA data source has already analyzed, review the number of sessions ESA would process after you edit the position tracking, and plan your work.
- Set the tracking position information based on:
  - Session ID
  - Date and Time (Collection Time)
- Set position tracking for multiple data sources before you deploy them.
- Calculate the number of sessions that the ESA Correlation Service is scheduled to process for a particular data source to either process, reprocess, or skip sessions with respect to the current position of the data source.

**Note:** The Position tracking feature with the Date and Time option works based on the profile time settings in the NetWitness Platform XDR UI. This time-zone based time from the UI is converted to UTC, and is sent to the core, to retrieve the corresponding session ID for that time stamp. Example: If the UI follows IST, the UI converts it to UTC and sends it to the core. The session ID is fetched for the specific UTC time stamp, and set to position tracking at deployment.

### Use Case Scenario

This section provides information about how you can use position tracking information in a real-world scenario.

**Case 1:** If you have deployed a data source with a total of 400 sessions that ESA has already processed, and if you want to start processing the events from the beginning, perform the following steps to reprocess the sessions.

#### Edit the position Tracking Information

1. Select the deployment and click **Edit Deployment**.
2. Select the datasource and click **Set Position Tracking Information**.

The Set Position Tracking Information dialog is displayed.

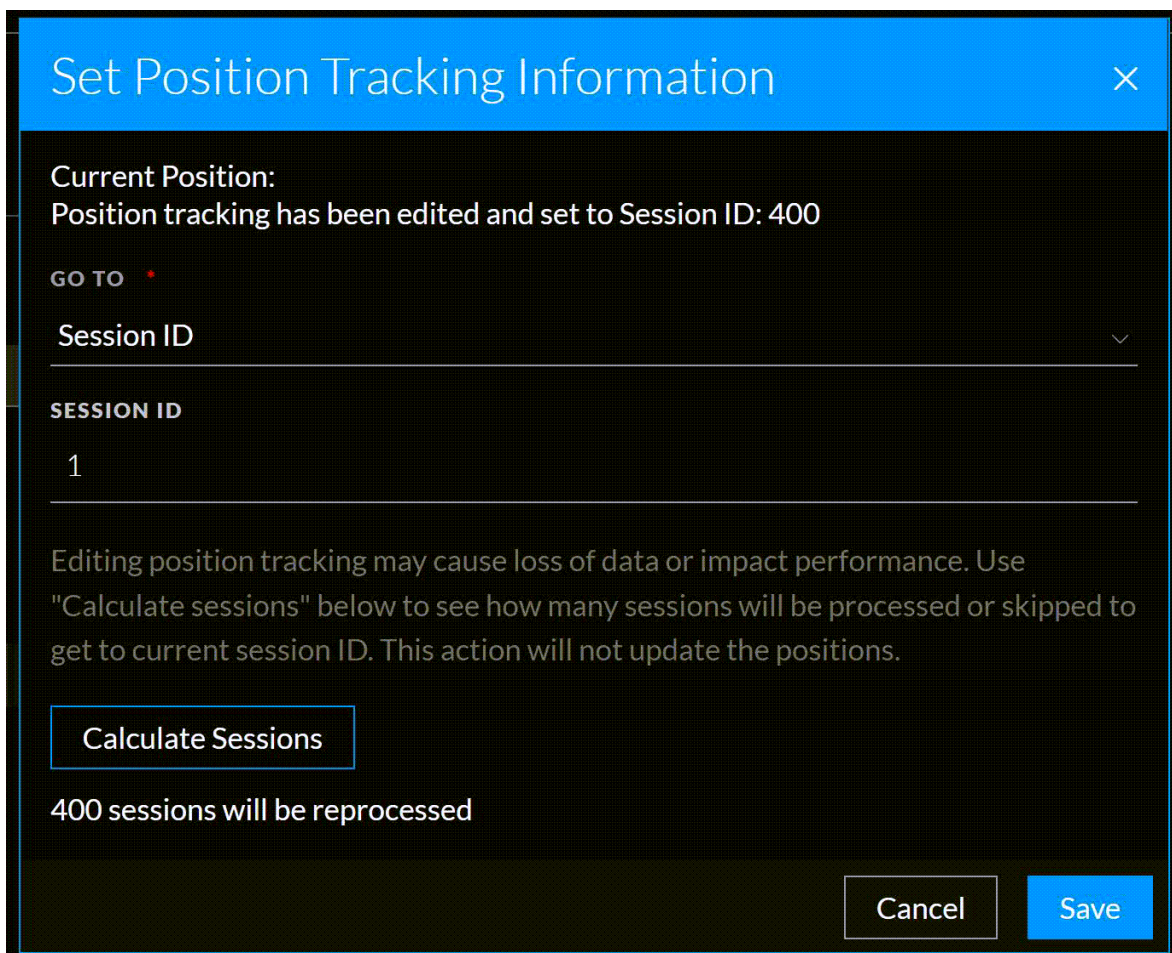
3. In the **Go To** drop-down menu, select the **Session ID** and enter the session number as 1 in the **Session ID** text field.

You can also set the position tracking information based on date and time and the sessions will be calculated using data and time.

4. Click **Calculate Sessions**.
5. Click **Save** twice.
6. Select the Deployment and click **Deploy**.

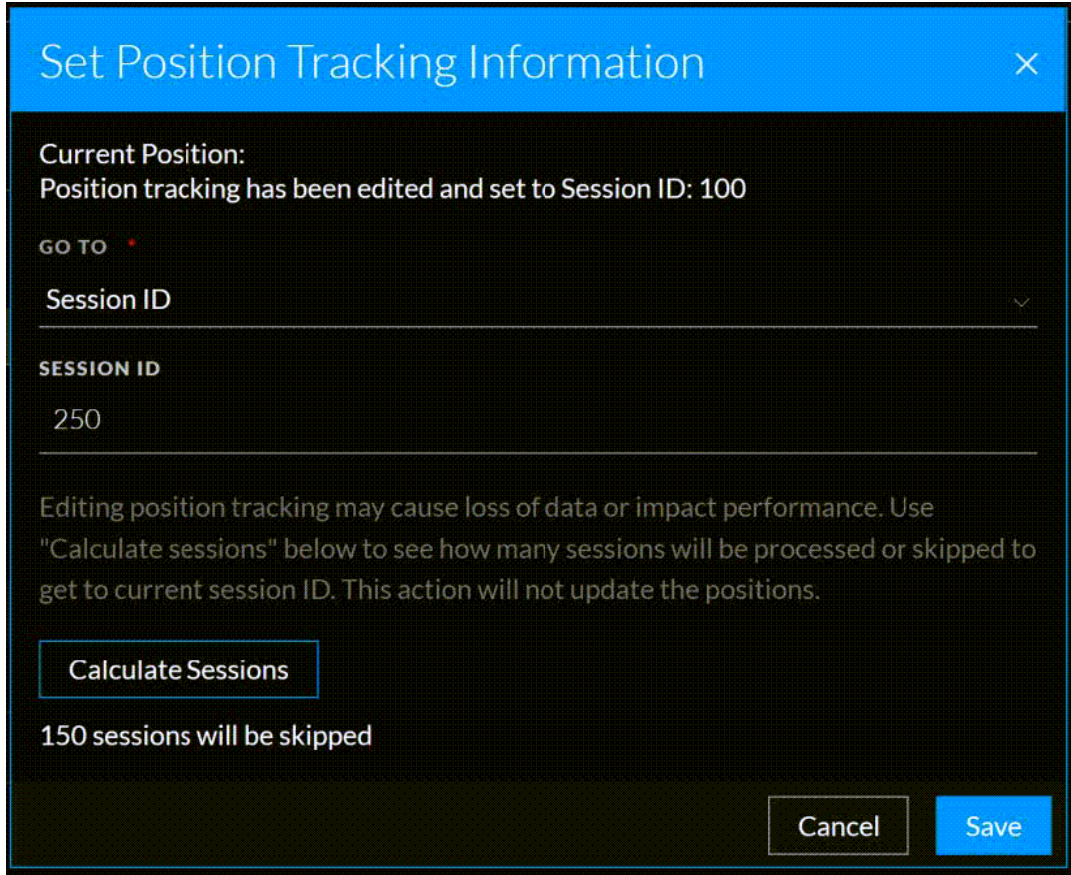
All the 400 sessions will be reprocessed.

The following image shows the use case scenario.



**Case 2:** If you have deployed a data source with a total of 700 sessions available and the current position of the data source is at 100 and if you set the sessions ID to 250. In this case, 150 sessions will be skipped. You can also set the sessions based on the date and time.

The following image shows the use case scenario.



**Case 3:** If you have deployed a data source that has a total of 1921237 sessions available and if you set the session ID higher than the available sessions for the data source. In this case, no remaining sessions will be processed. You can also set the sessions based on date and time.

The following image shows the use case scenario.

## Set Position Tracking Information ✕

**Current Position:**  
Position tracking has been edited and set to Session ID: 100

GO TO •

Session ID ▾

---

**SESSION ID**

1921245

---

Editing position tracking may cause loss of data or impact performance. Use "Calculate sessions" below to see how many sessions will be processed or skipped to get to current session ID. This action will not update the positions.

No sessions remaining to be processed

**Note:** Editing the tracking information is optional. If you add a new data source to an existing ESA deployment, and you do not edit the tracking information, ESA follows the default behavior to process events.