

# NetWitness<sup>®</sup> Platform XDR

Version 12.0

## 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 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.

November, 2022

# Contents

---

<b>Live Services Management</b>	<b>7</b>
NetWitness Live	7
NetWitness Feedback and Data Sharing	7
For Debian Linux and NetWitness Endpoint Users	7
<b>Deploy Content</b>	<b>8</b>
Create Live Account	9
Reset the Password for Your Live Account	12
Set Up Live Services on NetWitness	13
Deploy Content using Live Content UI	15
Live Services Required Procedures	16
Find and Deploy Live Resources	17
Find Resources in Live	17
Deploy Resources in Live	18
Manage Live Resources	23
Manage Subscription and Deployment	23
Remove a Deployed Resource	24
Deploy a Resource Bundle	24
Download Resources	24
Set Up Data Feeds	24
Search and Download Content from NetWitness XDR Cloud Services Live	25
Quick Search for Content	25
Advanced Search for Content	26
Download Content	27
Additional Procedures	29
Export Data to RSA	30
About Live Feedback	30
Download Live Feedback Historical Data	30
Share Telemetry Data to NetWitness	30
Packaging Resources	32
Create and Deploy Resource Package Use Case	32
Prerequisites to Create a Resource Package	32
Creating a Resource Package	32
Creating Threat Package	33
Deploying a Threat Package	34
Manage Custom Feeds	36
Custom Feed Creation	36
Sample Feed Definition File	36
Feed Definition Equivalents for Custom Feed Wizard Parameters	37
Creating a Custom Feed	40
Import Certificates for HTTPS Service	46

Create a STIX Custom Feed .....	48
MetaCallback Feeds using CIDR Index Range for IPv4 and IPv6 .....	53
Creating and Managing an Identity Feed .....	54
Import the SSL Certificate .....	61
Cannot Verify Identity Feed URL .....	61
Investigating an Identity Feed .....	62
Editing a Feed .....	64
Removing a Feed .....	66
Subscribing to Live Resources .....	68
Subscription Updates .....	68
Adding Subscribed Resources for Deployment to Services .....	69
Deleting a Subscription .....	69
Removing Subscribed Resources from the Deployments Subscriptions Grid .....	70
Subscribe and Unsubscribe to a Resource .....	70
Viewing Subscribed Resources Selected to Deploy on Services .....	72
Miscellaneous Live Services Procedures .....	73
Displaying Resource Details in Live Resource View .....	73
Downloading a Resource .....	74
Locating and Removing a Deployed Resource from Services .....	74
Showing Results as a List or in Detail .....	75
Viewing Resource Details .....	76
References .....	78
Live Configure View .....	79
Deployments Tab .....	80
Groups Panel .....	81
Subscriptions Panel .....	81
Subscriptions Tab .....	82
Toolbar .....	82
Grid .....	83
Discontinued Resources Tab .....	84
Groups Panel .....	84
Discontinued Resources on Service Panel .....	85
Live Feeds View .....	86
Toolbar .....	86
Feeds Grid .....	87
Live Resource View .....	88
Resource Details .....	88
Resource View Toolbar .....	89
Live Search View .....	91
Search Criteria Panel .....	91
Matching Resources Panel .....	93
Detailed Results .....	93



Grid Results .....	94
See Also .....	95
Live Search Content View .....	96
Search Content Panel .....	97
Search Results Panel .....	99
Content Details Panel .....	100
Resource Package Deployment Wizard .....	103
Features .....	103
Package Tab .....	103
Resources Tab .....	104
Services Tab .....	104
Review Tab .....	105
Deploy Tab .....	106
NetWitness Live Registration Portal .....	108
NetWitness Feedback and Data Sharing .....	110
Additional Live Services .....	110
Live Feedback .....	110
File Reputation .....	110
Troubleshooting Live Services .....	112
OutOfMemoryError on Context Hub Server .....	112
Troubleshooting Live Connect Threat Data Sharing .....	112
Query Log Retrieval Sample .....	113
System Logging: Debug .....	113
Policy-based Centralized Content Management .....	115
About Policy-based Centralized Content Management .....	117
Migrate Content from Core Services to Content Library .....	119
About Content Library .....	121
Import Content to Content Library .....	121
Create an Application Rule .....	122
Edit Application Rule .....	122
Delete Application Rule .....	123
View Application Rule Details .....	123
Create a Network Rule .....	123
Edit Network Rule .....	124
Delete Network Rule .....	124
View Network Rule Details .....	125
About Groups .....	125
Create a Group .....	125
View a Group .....	126
Delete a Group .....	126
Edit a Group .....	127
About Policies .....	127

Create and Publish Policies .....	128
Clone a Policy .....	129
Delete a Policy .....	130
Edit a Policy .....	130
View a Policy .....	131
Enable Content for a Policy .....	132
Disable Content for a Policy .....	132
References .....	132
Content Library Tab .....	132
Groups Tab .....	134
Policies Tab .....	138
Appendix A: Endpoint Risk Scoring Rules .....	142

# Live Services Management

---

RSA 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 RSA 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

---

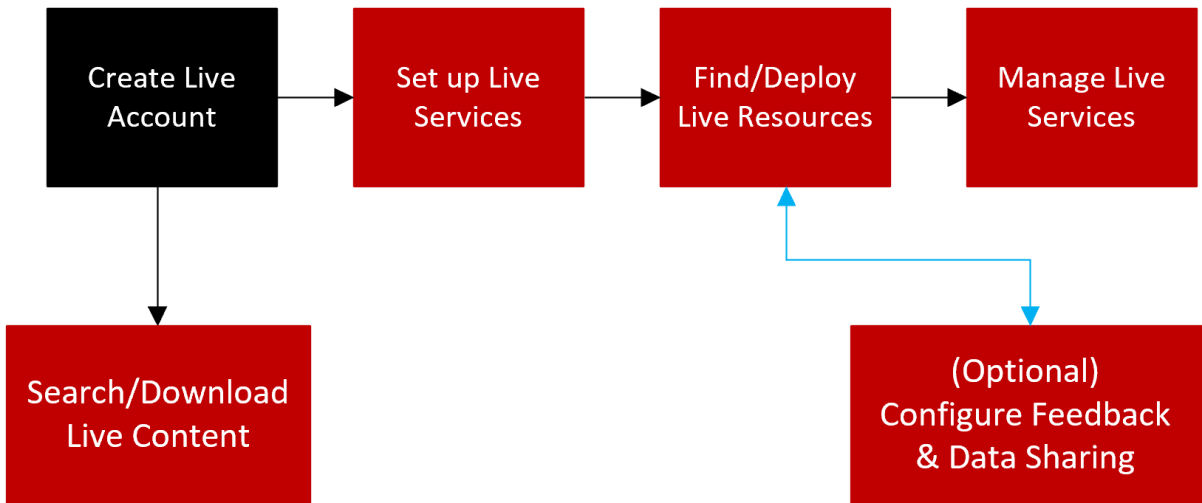
This section explains the different ways available to deploy content:

- [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 \*

Enter your username

Password \*

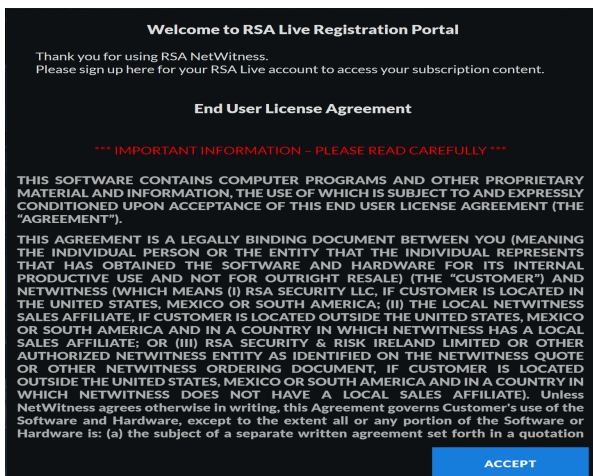
Enter your password \*

**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 image shows a web form for signing up for a NetWitness Live Account. The form is titled "Sign Up for NetWitness Live Account" with a help icon. It contains several input fields with 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]), and Password (Number,lower,UPPER, ~!@#\$%^&\*()-\_+=/; Length:[8,24]). At the bottom, 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.

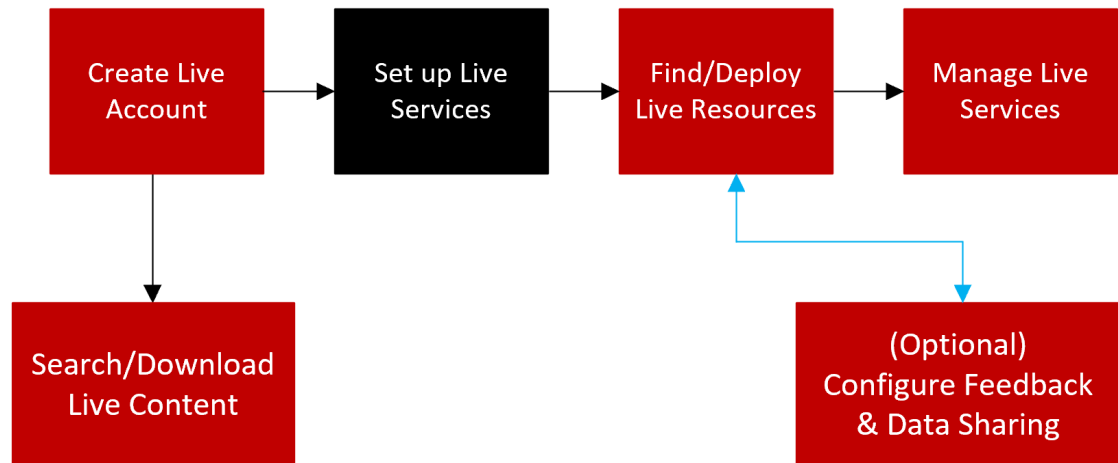
The image shows the NetWitness XDR Cloud Services Live sign up page. At the top, there is a logo with a red network icon and the text "NETWITNESS" in white, with "XDR Cloud Services" in red below it. The background is dark blue with a faint grid and glowing nodes. Below the logo, the text "Sign in with your username and password" is displayed. There are two input fields: "Username \*" with a placeholder "Enter your username" and "Password \*" with a placeholder "Enter your password". At the bottom, there are two buttons: a blue "SIGN IN" button and a white "SIGN UP FOR LIVE" button. To the right of the "SIGN UP FOR LIVE" button is a link that says "Forgot Password?".

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**.




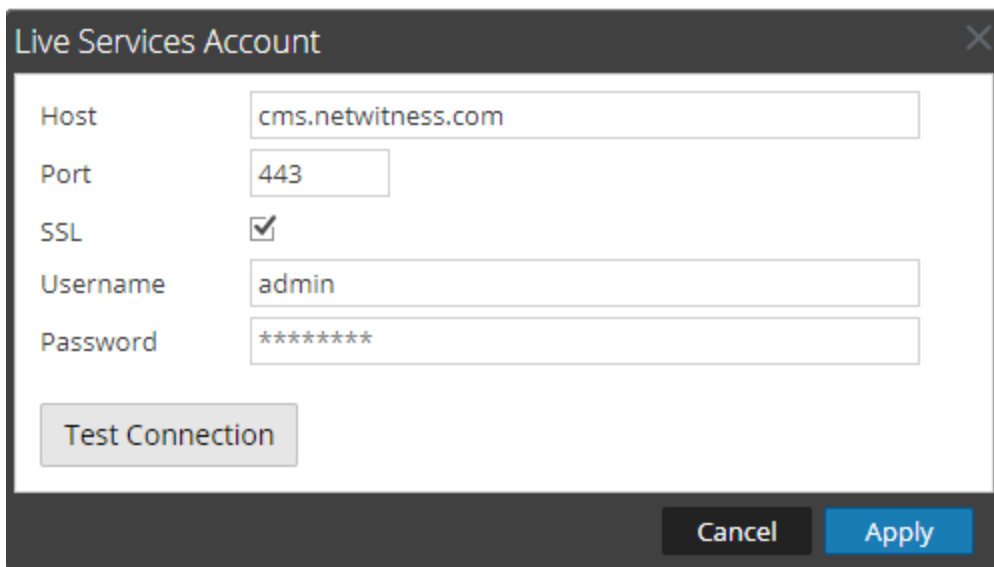
## Set Up Live Services on NetWitness

To set up Live on NetWitness, 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.



The 'Live Services Account' dialog box is shown. It contains the following fields and controls:

- Host:** cms.netwitness.com
- Port:** 443
- SSL:** ☒
- Username:** admin
- Password:** \*\*\*\*\*
- Test Connection:** A button to verify the connection.
- Cancel:** A button to close the dialog without saving.
- Apply:** A button to save the configuration.

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 with updates from Cloud Services Live.

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

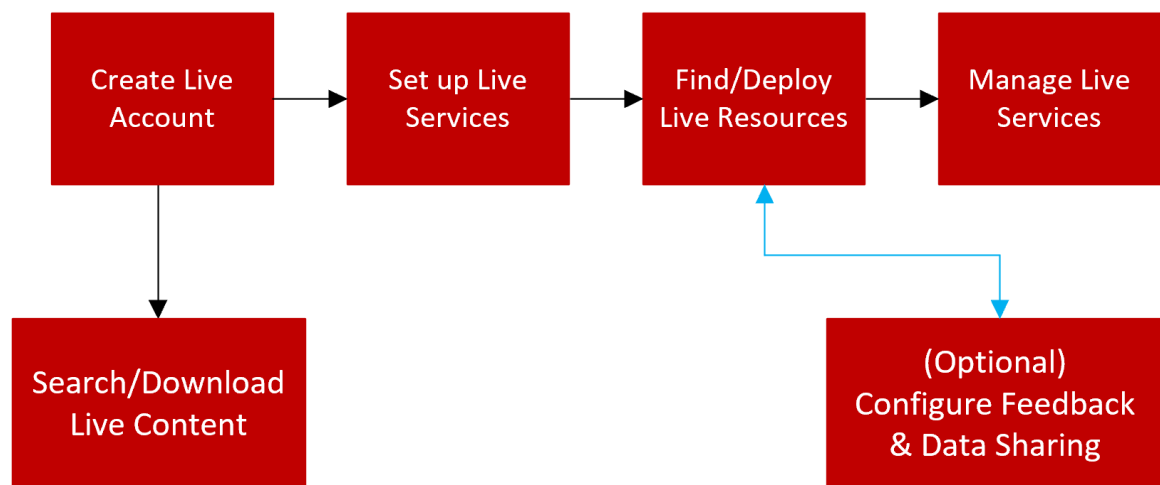
## Deploy Content using Live Content UI

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

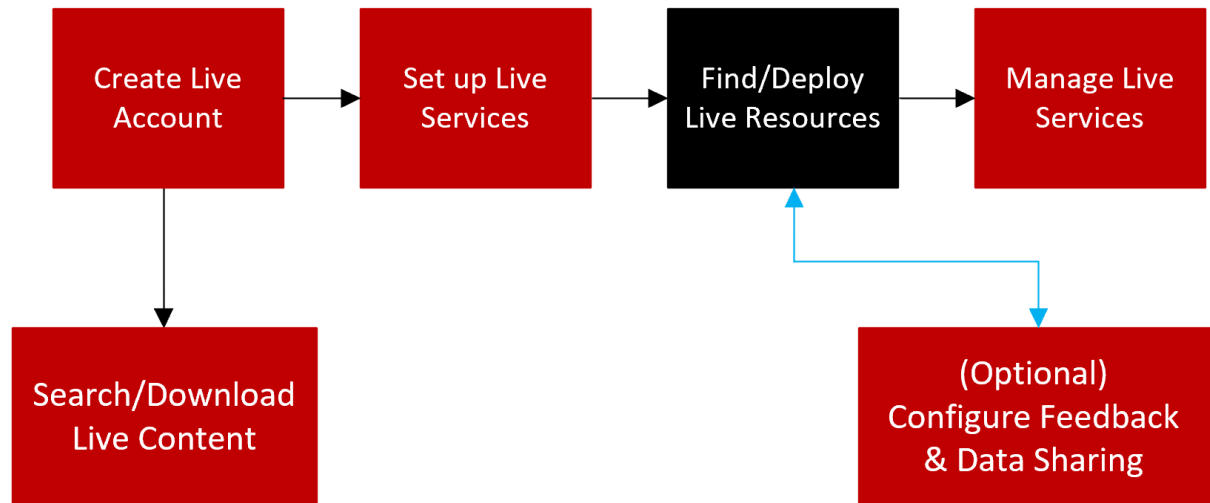
The following workflow describes the basic setup into four steps, which you perform individually.



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> . If you have an existing account, you can manage your account using this portal.
<a href="#">Set Up Live Services on NetWitness</a>	Set Up Live Services on NetWitness 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

To find resources:

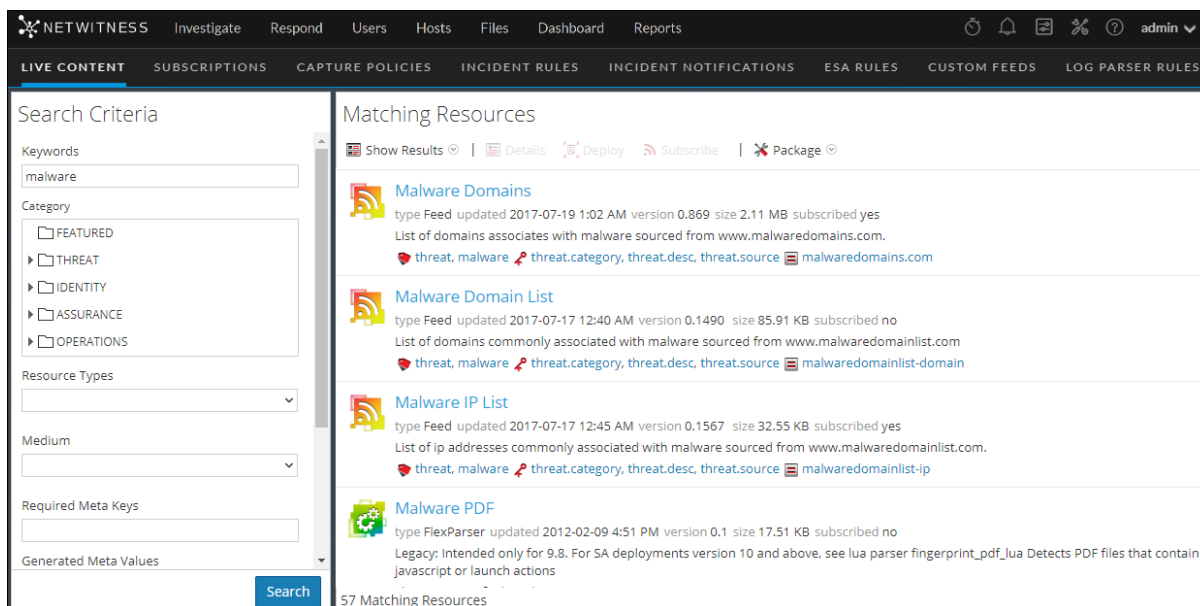
1. Navigate to  **(Configure) > Live Content**.
2. In the **Search Criteria** panel, specify search criteria. Enter any or all of these: keyword, category, type of resource, medium, meta keys, meta values, date resource was created, and date resource was modified.

The screenshot shows the 'Search Criteria' panel with the following fields and options:

- Keywords:** A text input field.
- Category:** A list of categories with expandable arrows: ☐ FEATURED, ☐ THREAT, ☐ IDENTITY, ☐ ASSURANCE, and ☐ OPERATIONS.
- Resource Types:** A dropdown menu.
- Medium:** A dropdown menu.
- Required Meta Keys:** A text input field.
- Generated Meta Values:** A text input field.
- Resource Created Date:** Two date pickers labeled 'Start Date' and 'End Date'.
- Resource Modified Date:** A text input field.
- Search:** A blue button at the bottom right.

### 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.

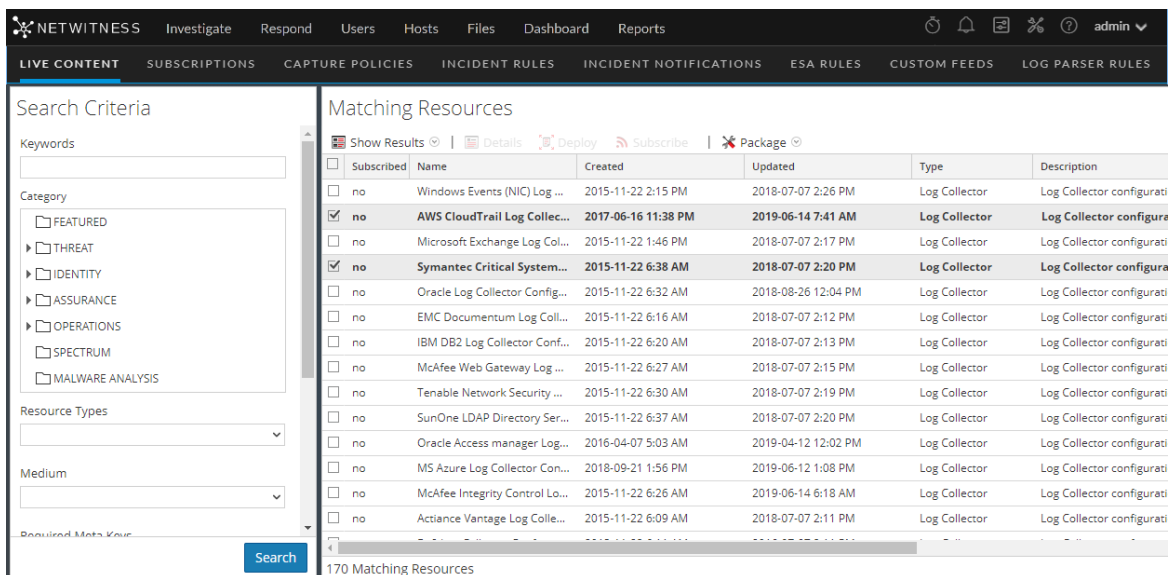
**Caution:** For NetWitness 11.3, there is a new Content bundle for Endpoint, which contains approximately 400 application rules. Do not deploy this bundle (or the Endpoint application rules) onto any Log Decoder that is running an earlier version of NetWitness. The rules are only useful for 11.3 and 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.

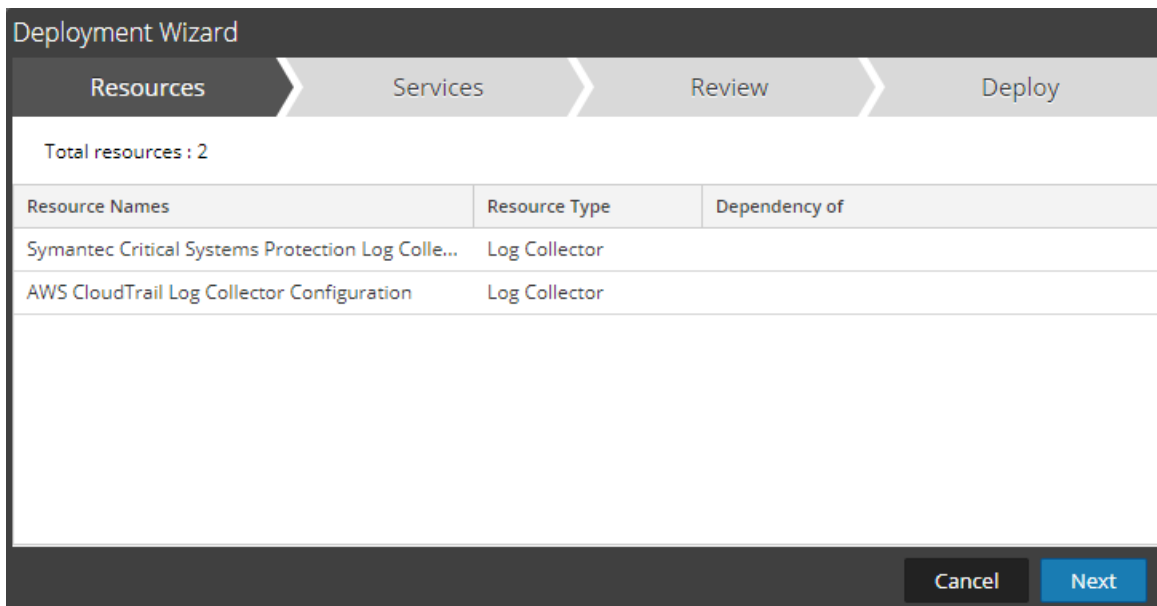


The screenshot shows the NETWITNESS interface with the **LIVE CONTENT** tab selected. On the left, the **Search Criteria** panel shows filters for Category (Threat, Identity, Assurance, Operations, Spectrum, Malware Analysis) and Resource Types. The **Matching Resources** panel on the right displays a table of resources.

Subscribed	Name	Created	Updated	Type	Description
<input type="checkbox"/>	Windows Events (NIC) Log ...	2015-11-22 2:15 PM	2018-07-07 2:26 PM	Log Collector	Log Collector configurati
<input checked="" type="checkbox"/>	AWS CloudTrail Log Collec...	2017-06-16 11:38 PM	2019-06-14 7:41 AM	Log Collector	Log Collector configura
<input type="checkbox"/>	Microsoft Exchange Log Col...	2015-11-22 1:46 PM	2018-07-07 2:17 PM	Log Collector	Log Collector configurati
<input checked="" type="checkbox"/>	Symantec Critical System...	2015-11-22 6:38 AM	2018-07-07 2:20 PM	Log Collector	Log Collector configura
<input type="checkbox"/>	Oracle Log Collector Config...	2015-11-22 6:32 AM	2018-08-26 12:04 PM	Log Collector	Log Collector configurati
<input type="checkbox"/>	EMC Documentum Log Coll...	2015-11-22 6:16 AM	2018-07-07 2:12 PM	Log Collector	Log Collector configurati
<input type="checkbox"/>	IBM DB2 Log Collector Conf...	2015-11-22 6:20 AM	2018-07-07 2:13 PM	Log Collector	Log Collector configurati
<input type="checkbox"/>	McAfee Web Gateway Log ...	2015-11-22 6:27 AM	2018-07-07 2:15 PM	Log Collector	Log Collector configurati
<input type="checkbox"/>	Tenable Network Security ...	2015-11-22 6:30 AM	2018-07-07 2:19 PM	Log Collector	Log Collector configurati
<input type="checkbox"/>	SunOne LDAP Directory Ser...	2015-11-22 6:37 AM	2018-07-07 2:20 PM	Log Collector	Log Collector configurati
<input type="checkbox"/>	Oracle Access manager Log...	2016-04-07 5:03 AM	2019-04-12 12:02 PM	Log Collector	Log Collector configurati
<input type="checkbox"/>	MIS Azure Log Collector Con...	2018-09-21 1:56 PM	2019-06-12 1:08 PM	Log Collector	Log Collector configurati
<input type="checkbox"/>	McAfee Integrity Control Lo...	2015-11-22 6:26 AM	2019-06-14 6:18 AM	Log Collector	Log Collector configurati
<input type="checkbox"/>	Actiance Vantage Log Colle...	2015-11-22 6:09 AM	2018-07-07 2:11 PM	Log Collector	Log Collector configurati

170 Matching Resources

- d. In the Matching Resources toolbar, click .



The screenshot shows the **Deployment Wizard** with the **Resources** step selected. It displays a table of resources to be deployed.

Resource Names	Resource Type	Dependency of
Symantec Critical Systems Protection Log Colle...	Log Collector	
AWS CloudTrail Log Collector Configuration	Log Collector	

Buttons: Cancel, Next

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.

The screenshot shows the 'Resource Package Deployment' wizard with a progress bar at the top containing five steps: Package, Resources, Services, Review, and Deploy. The 'Package' step is currently active. Below the progress bar, there is a label 'Resource Bundle' followed by a text input field and a 'Browse' button. At the bottom right of the wizard, there are 'Cancel' and 'Next' buttons.


- 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.



The screenshot shows the 'Deployment Wizard' interface with the 'Services' step selected. The wizard has four steps: Resources, Services, Review, and Deploy. Below the step indicators, there are two tabs: 'Services' (active) and 'Groups'. A table lists available services with checkboxes and green leaf icons. The table has columns for 'Name' and 'Type'.

<input type="checkbox"/>		Name ^	Type
<input type="checkbox"/>		UI Endpoint	Other

At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

6. Click **Next**.

The **Review** page is displayed.

The screenshot shows the 'Deployment Wizard' interface with the 'Review' step selected. The wizard has four steps: Resources, Services, Review, and Deploy. Below the step indicators, there is a table summarizing the deployment configuration. The table has four columns: 'Service', 'Service Type', 'Resource Name', and 'Resource Type'.

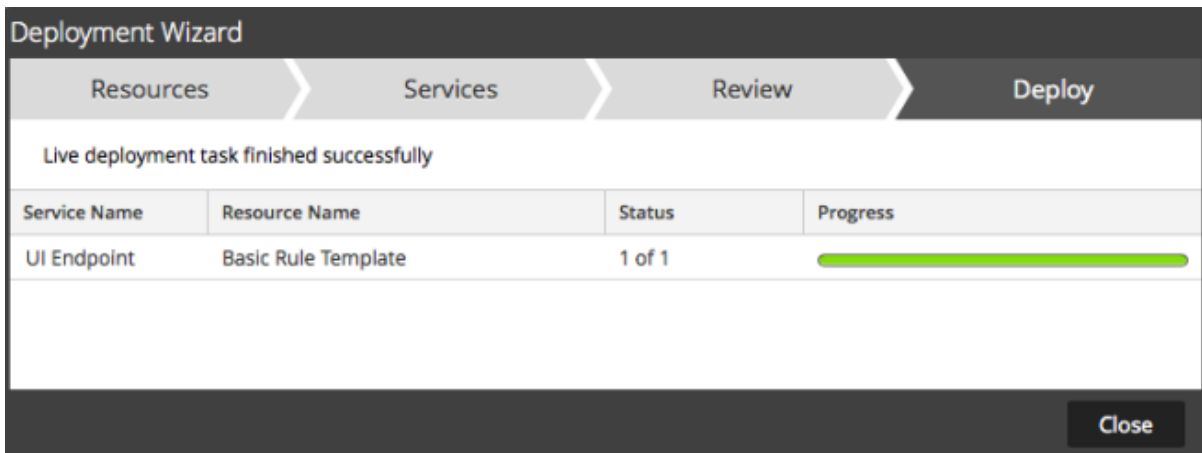
Service	Service Type	Resource Name	Resource Type
UI Endpoint	NW Local	Basic Rule Template	RSA Event Stream Analy...

At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Deploy'.

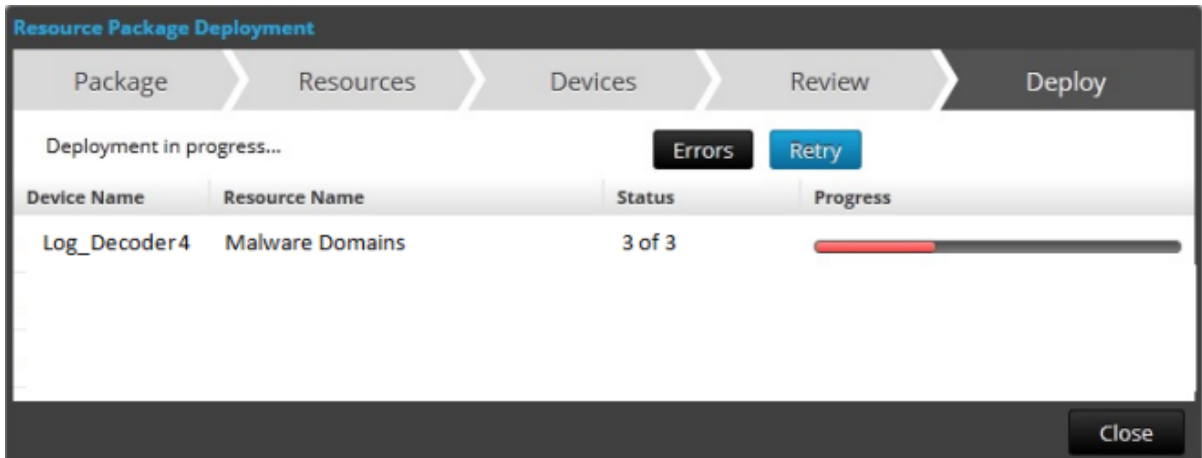
Make sure that you have selected correct resources and the services on which you want to deploy them.

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.




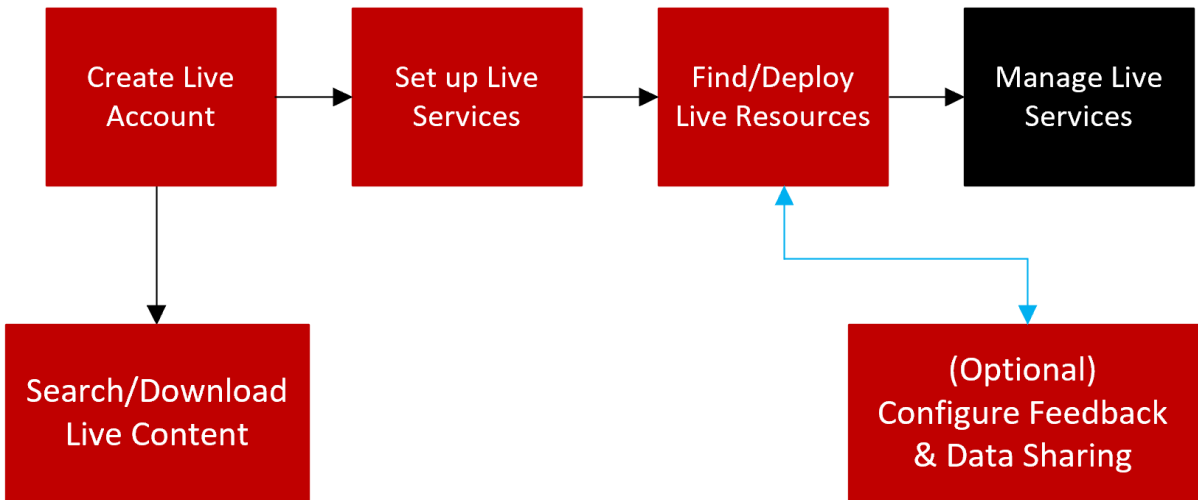
8. Click **Close**.

### 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.

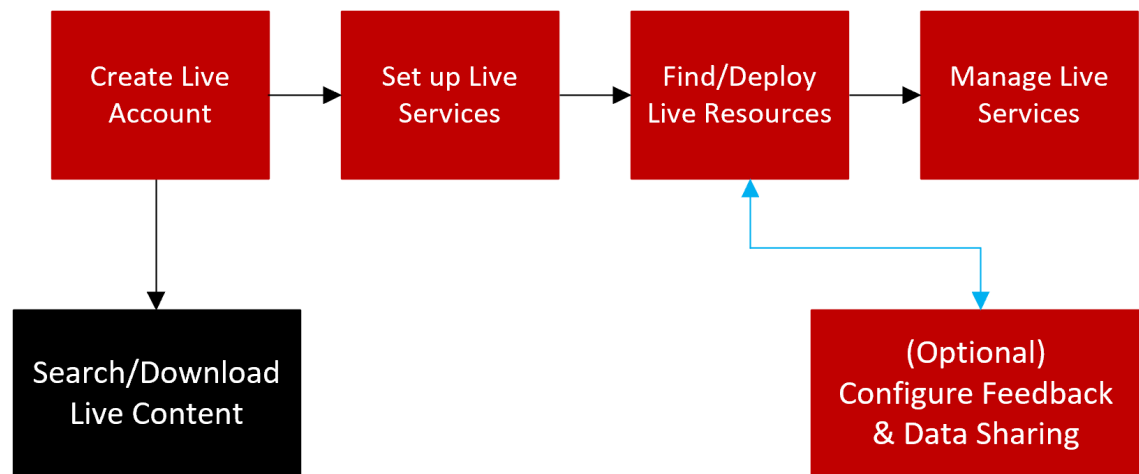
**Set Up Data Feeds**

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.

**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:

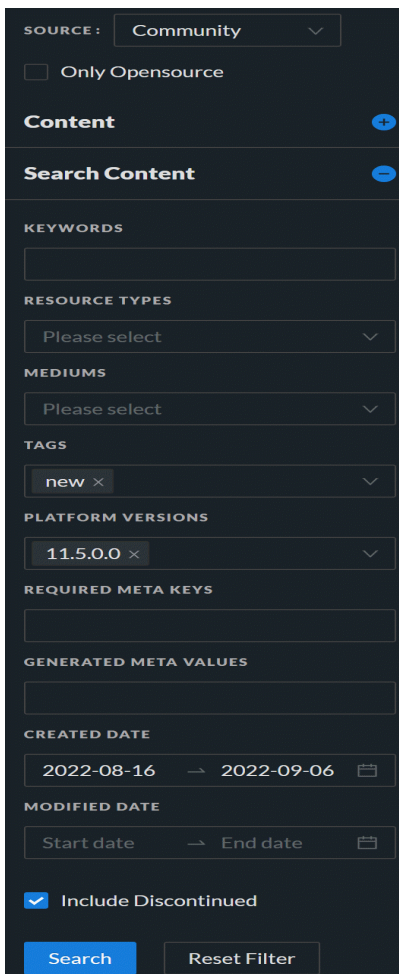
- **New:** Displays the content which is created in the last 21 days.
- **Recently Updated:** Displays the content which is created or updated in the last 21 days.

## 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.



SOURCE: Community

☐ Only Opensource

**Content** 

**Search Content** 

KEYWORDS

RESOURCE TYPES

Please select

MEDIUMS

Please select

TAGS

new

PLATFORM VERSIONS

11.5.0.0

REQUIRED META KEYS

GENERATED META VALUES

CREATED DATE

2022-08-16 → 2022-09-06


MODIFIED DATE

Start date → End date

☒ Include Discontinued

Search Reset Filter

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 ▾
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

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 the right panel by performing the following steps:

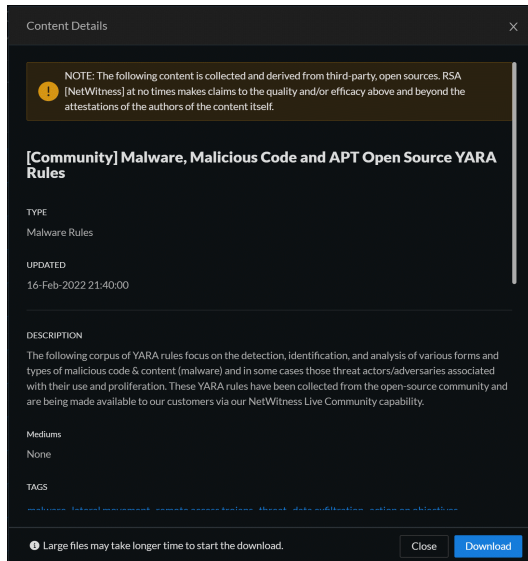
**Note:**

- You cannot download a discontinued content.
- 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 content:

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

The **Content Details** dialog is displayed.



2. Click **Download**.

The content file is downloaded.



## 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:

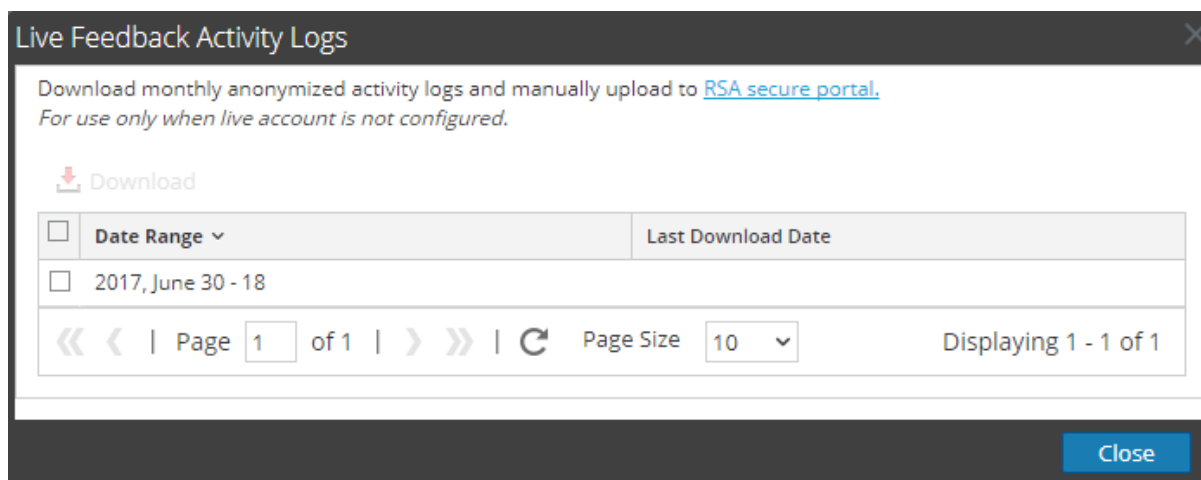
1. Go to  (Admin) > System.

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

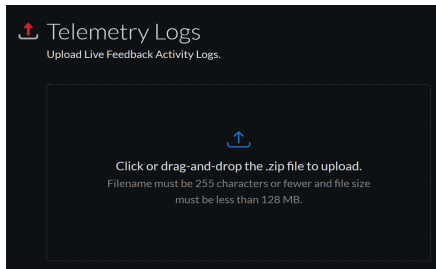
After you download the Live Feedback data, you can then upload it using the following procedure.

**Note:**

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

**To share the data to RSA:**

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.

The screenshot shows the NetWitness Live Content interface. On the left, the 'Search Criteria' pane has the 'THREAT' category selected under 'Category'. The 'Matching Resources' pane on the right displays a table of resources. The table has columns for 'Name', 'Type', and 'Description'. The resources listed include various rules and reports such as 'Aggressive Internal Database Scan', 'Aggressive Internal NetBIOS scan', 'Alert IDs By Profiled Source IP', 'Alerts By Profiled Source IP', 'All Risk Suspicious', 'All Risk Suspicious by Destination...', 'All Risk Suspicious by Session Size', 'All Risk Suspicious by Source IP', 'All Risk Warning', 'All Risk Warning by Destination IP', 'All Risk Warning by Session Size', 'All Risk Warning by Source IP', 'apt\_artifacts', 'Archive From IP Address', 'Backdoor Activity Detected', and 'Behaviors of Compromise'. At the bottom of the Matching Resources pane, it says '233 Matching Resources'.

4. Select Package > Create.

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

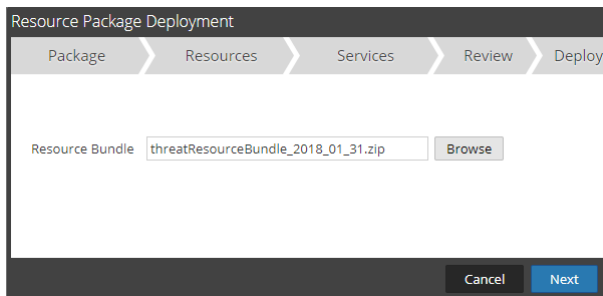
5. Rename the package to something meaningful. For example, in this case, you could change the package name to **threatResourceBundle\_2018\_01\_31.zip** (assuming today's date is January 31, 2018).

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.



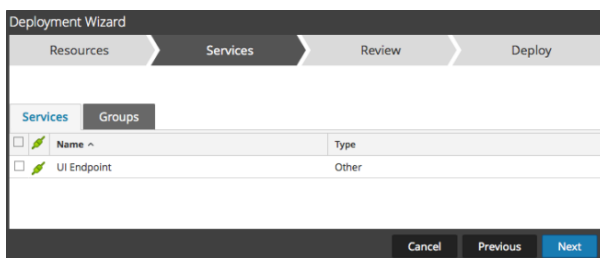
4. Click **Next**.

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" datatype="Text" />
        <LanguageKey name="threat.desc" datatype="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 tab</b>	
<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 tab - Advanced Options</b>	
<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>	Select the services to which you want to send the data feed.
(Define Columns tab, Define Index) <b>Type</b>	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.

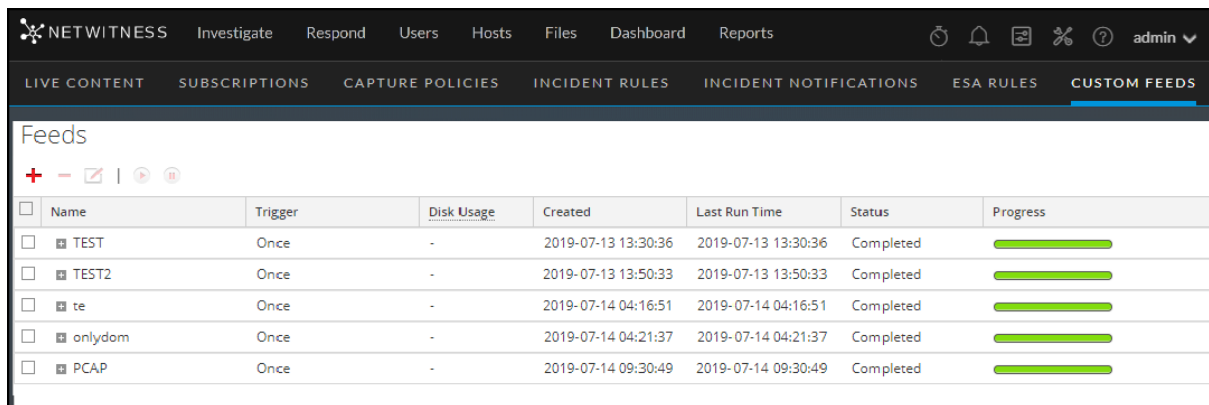
The feed data file (.csv or STIX (.xml)) and optionally the feed definition file (.xml) must be available on the local file system for an on-demand custom feed. For a recurring custom feed, the files must be available at a URL that is accessible to the NetWitness server.

**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.

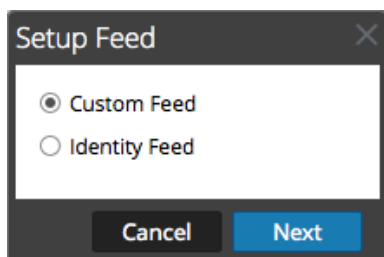
The Custom Feeds view is displayed.



	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>

2. In the toolbar, click .

The Setup Feed dialog is displayed.



Setup Feed

☒ Custom Feed

☐ Identity Feed

Cancel Next

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

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

The screenshot shows the 'Configure a Custom Feed' wizard with the 'Define Feed' step active. The wizard has four tabs: 'Define Feed', 'Select Services', 'Define Columns', and 'Review'. In the 'Define Feed' tab, the 'Feed Type' is set to 'CSV' (selected with a radio button) and 'STIX' is unselected. The 'Feed Task Type' is set to 'Adhoc' (selected with a radio button) and 'Recurring' is unselected. There is a 'Name \*' text field. Below it, the 'Upload As Csv File Feed' checkbox is unchecked. There is a 'File \*' text field with a 'Select File' button and a 'Browse' button. At the bottom left, there is a link for 'Advanced Options'. At the bottom right, there are 'Reset', 'Cancel', 'Prev', and 'Next' buttons.

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

The Advanced Options are displayed:

This screenshot is similar to the previous one but with the 'Advanced Options' section expanded. It shows additional fields: 'XML Feed File' with a 'Select File' button and a 'Browse' button, a 'Separator' dropdown menu currently set to ',', and a 'Comment' dropdown menu currently set to '#'. The 'Reset', 'Cancel', 'Prev', and 'Next' buttons remain at the bottom.

- e. 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**.
- f. 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.

<input type="checkbox"/>	Name ^	Address	Type
<input type="checkbox"/>	[Redacted]	[Redacted]	Decoder
<input type="checkbox"/>	[Redacted]	[Redacted]	Decoder
<input type="checkbox"/>	[Redacted]	[Redacted]	Decoder
<input type="checkbox"/>	[Redacted]	[Redacted]	Log Decoder
<input type="checkbox"/>	[Redacted]	[Redacted]	Decoder
<input type="checkbox"/>	[Redacted]	[Redacted]	Log Decoder
<input type="checkbox"/>	[Redacted]	[Redacted]	Decoder
<input type="checkbox"/>	[Redacted]	[Redacted]	Decoder
<input type="checkbox"/>	[Redacted]	[Redacted]	Decoder
<input type="checkbox"/>	[Redacted]	[Redacted]	Log Decoder
<input type="checkbox"/>	[Redacted]	[Redacted]	Log Decoder
<input type="checkbox"/>	[Redacted]	[Redacted]	Decoder
<input type="checkbox"/>	[Redacted]	[Redacted]	Decoder
<input type="checkbox"/>	[Redacted]	[Redacted]	Log Decoder
<input type="checkbox"/>	[Redacted]	[Redacted]	Log Decoder

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.

Configure a Custom Feed

Define Feed | Select Services | Define Columns | Review

Feed Type: ☒ CSV ☐ STIX

Feed Task Type: ☐ Adhoc ☒ Recurring

Name \*: TestFeed

Upload As Csv File Feed: ☐

URL \*: [Text Field] [Verify]

☐ Authenticated

☐ Use Proxy

Recur Every: [Dropdown]

☐ Date Range

Advanced Options

XML Feed File: [Text Field] [Browse]

Separator: [Text Field]

Comment: #

- 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 'Authenticated' and 'Use proxy' checkboxes are unchecked. The 'Recur Every' field is set to '3' and 'Day(s)'. The 'Date Range' section is collapsed. The 'Advanced Options' section is expanded, showing the 'XML Feed File' field with a 'Browse' button, the 'Separator' field set to a comma, and the 'Comment' field set to a hash. The dialog has 'Reset', 'Cancel', 'Prev', and 'Next' buttons at the bottom.

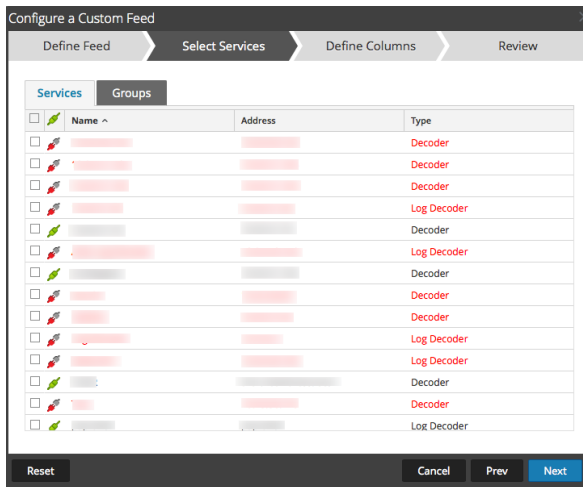
7. (Conditional) If you want to define a feed based on an XML feed file:

- 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.



Configure a Custom Feed

Define Feed > Select Services > Define Columns > Review

**Define Index**

Type ☐ IP ☐ IP Range ☒ Non IP

Index Column  Service Type  ☒ Truncate Domain ☐ Ignore Case

Callback Key (S)

**Define Values**

Column	1 (Index)
Key	OS
SRM_SaaS	access.point
ANCESTOR	accesses
	action
	alert
	alert.id
	alias.host
	alias.ip
	alias.ipv6
	alias.mac
	asn.dst
	asn.src
	attachment

Reset Cancel Prev Next

- 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.

Configure a Custom Feed

Define Feed > Select Services > Define Columns > Review

**Define Index**

Type ☐ IP ☐ IP Range ☒ Non IP


Index Column  Service Type  ☒ Truncate Domain ☐ Ignore Case

Callback Key (S)

**Define Values**

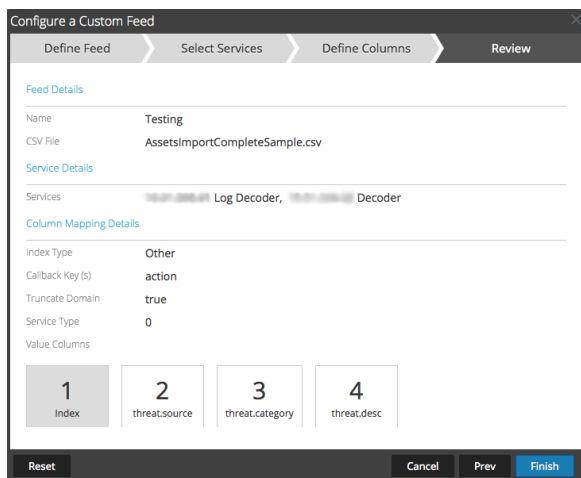
Column	1 (Index)	2	3	4
Key		threat.source	threat.category	threat.desc
SRM_SaaS_ES		MXASSETInterface	AddChange	EN
ANCESTOR		ASSETNUM	ASSETTAG	ASSETTYPE
		cent45	9164	
		cent45	9164	

Reset Cancel Prev Next

**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, 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>.

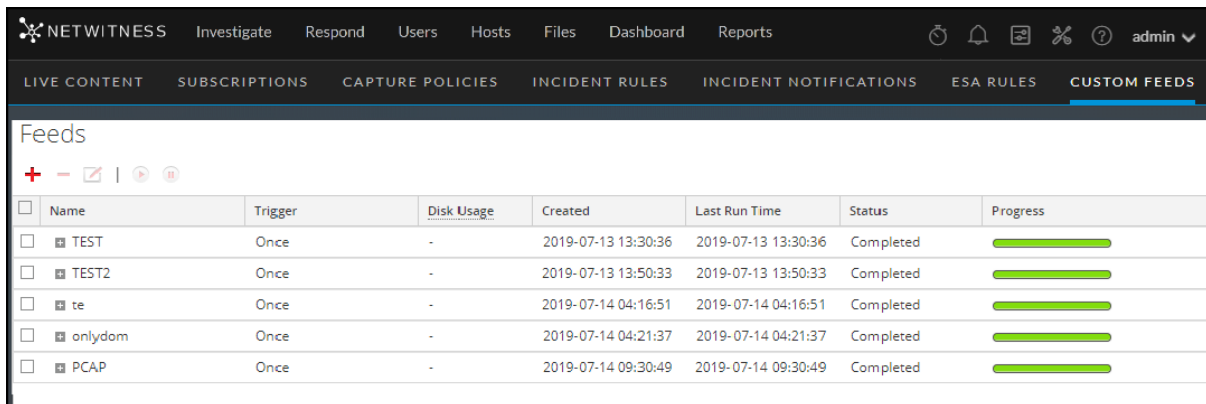
The feed data file (.csv or STIX (.xml)) and optionally the feed definition file (.xml) must be available on the local file system for an on-demand custom feed. For a recurring custom feed, the files must be available at a URL that is accessible to the NetWitness server.

In NetWitness Platform, 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.

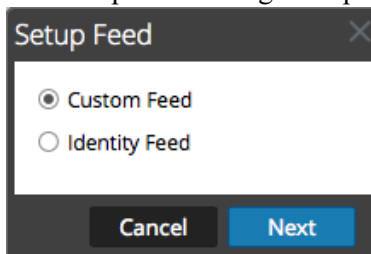
The Custom Feeds view is displayed.



	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></div>
<input type="checkbox"/>	TEST2	Once	-	2019-07-13 13:50:33	2019-07-13 13:50:33	Completed	<div></div>
<input type="checkbox"/>	te	Once	-	2019-07-14 04:16:51	2019-07-14 04:16:51	Completed	<div></div>
<input type="checkbox"/>	onlydom	Once	-	2019-07-14 04:21:37	2019-07-14 04:21:37	Completed	<div></div>
<input type="checkbox"/>	PCAP	Once	-	2019-07-14 09:30:49	2019-07-14 09:30:49	Completed	<div></div>

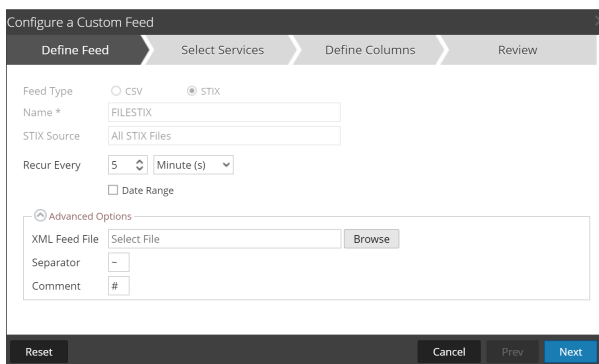
- In the toolbar, click .

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.



Configure a Custom Feed

Define Feed | Select Services | Define Columns | Review

Feed Type: ☐ CSV ☒ STIX

Name \*: FILESTIX

STIX Source: All STIX Files

Recur Every: 5 Minute(s)

☐ Date Range

Advanced Options

XML Feed File: Select File

Separator: -

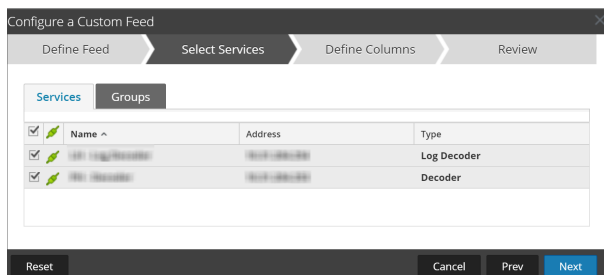
Comment: #

- 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.

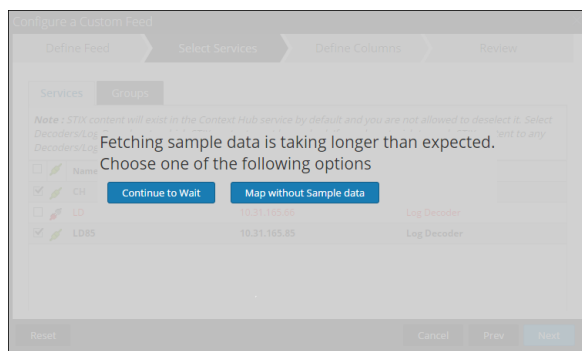
- Date Range:** Select the checkbox and specify the date range for the feed task to recur.

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
<input type="checkbox"/> 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></div>
<input type="checkbox"/> 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></div>
<input type="checkbox"/> 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></div>
<input type="checkbox"/> 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></div>
<input type="checkbox"/> TAXII Server1	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></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>
  </FlatFileFeed>
  <LanguageKeys>
    <LanguageKey name="alert" valuetype="Text" />
  </LanguageKeys>
  <Fields>
    <Field index="1" type="index" range="cidr"/>
    <Field index="2" type="value" key="alert" />
  </Fields>
</FDF>
```

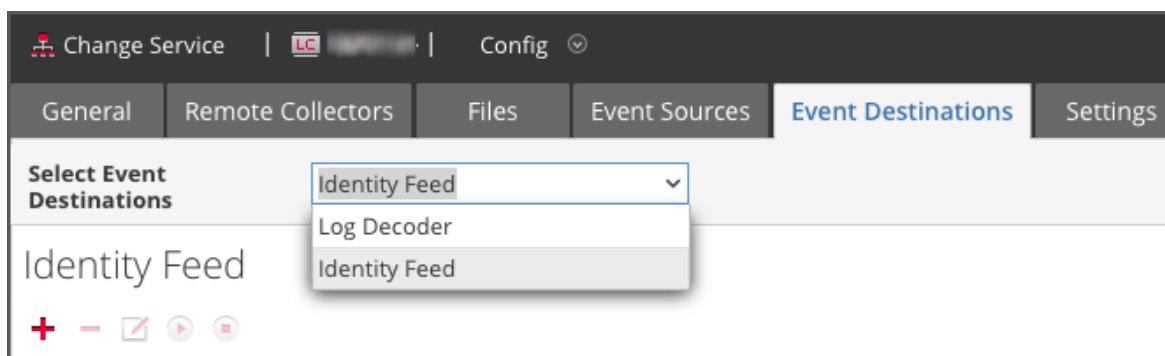
**Note:** To configure a CIDR index range for feeds with single or multiple MetaCallbacks of value type IPv4 or IPv6, the field of type index MUST contain a range attribute with range="cidr". Also, configuring "cidr" index ranges for feeds with MetaCallbacks of multiple different value types is not supported.


## 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.

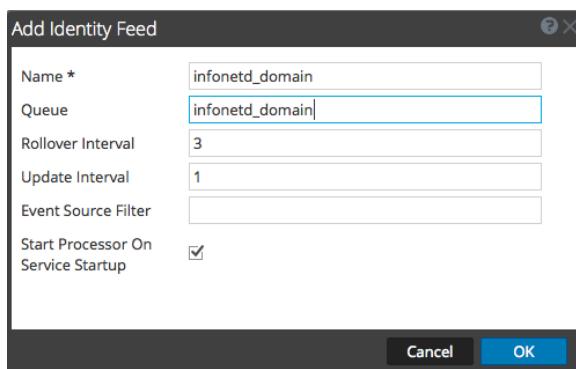
### To create an identity feed:

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.



- 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.

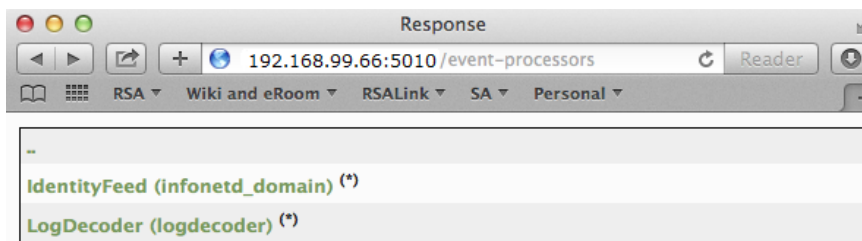
- b. Verify that data is written to the feed files. SSH to the Log Decoder/Collector or Virtual Log Collector being configured. Navigate to `/var/netwitness/logcollector/runtime/identity-feed` and verify that the `Identity_deploy` files are getting populated with data.

```
[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**

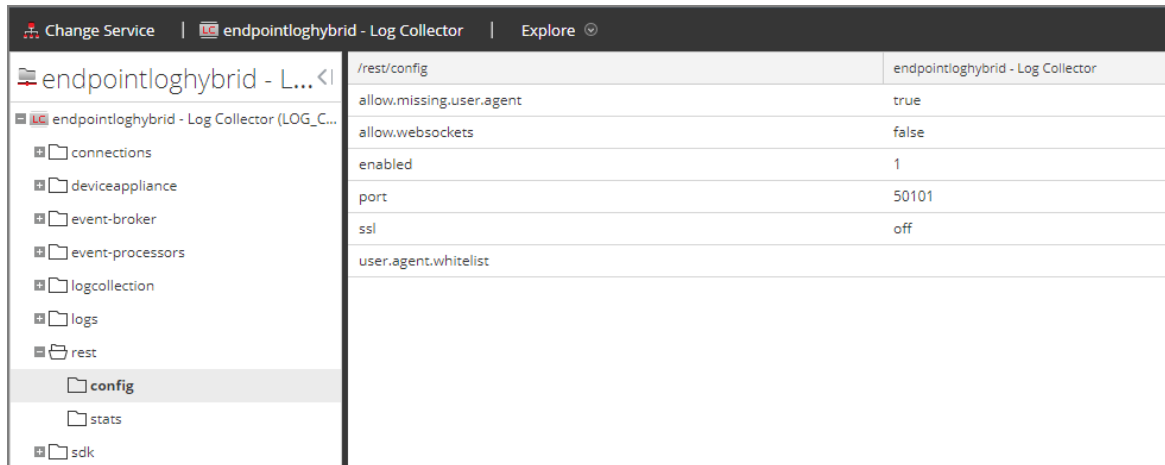
The browser screen should look like this:



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**.



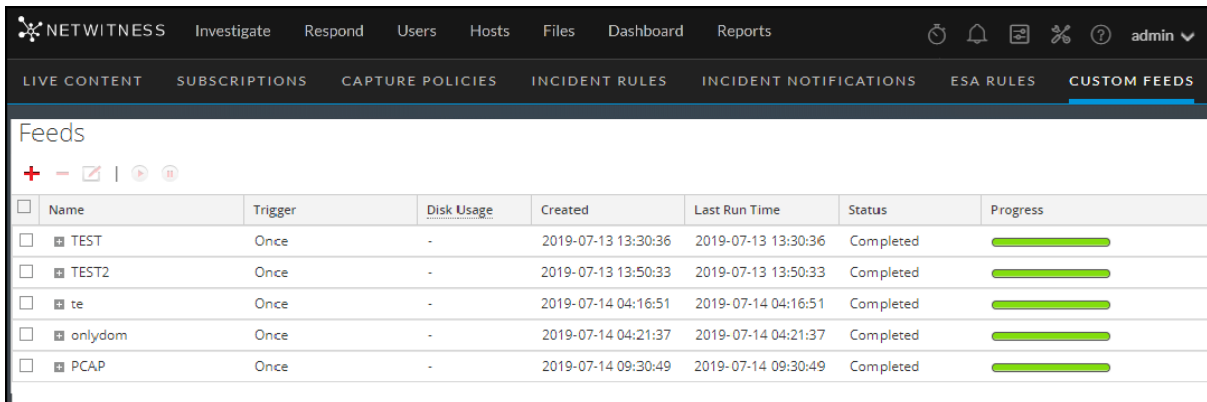
For REST to be active, **enabled** must be set to **1**.

- 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.

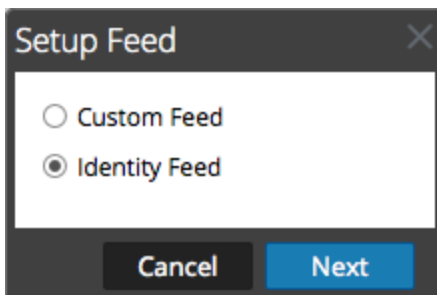
3. Go to  **(Configure) > Custom Feeds**.

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.

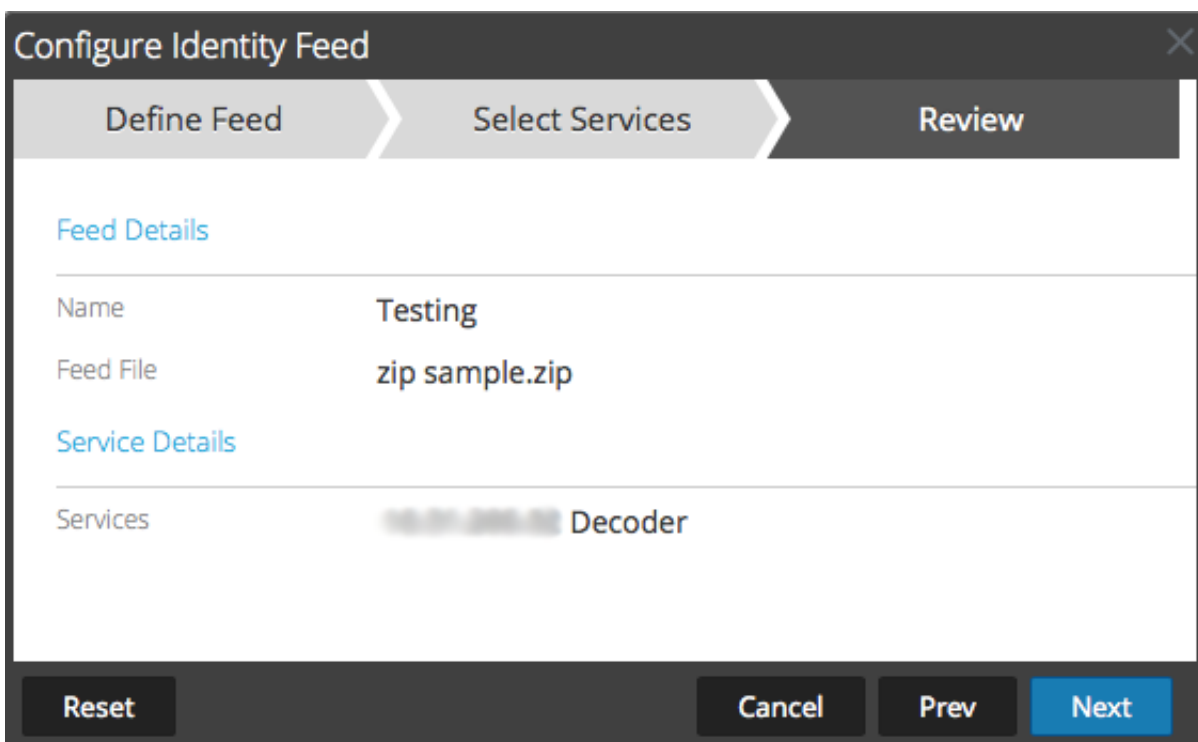
The screenshot shows the 'Configure Identity Feed' dialog box with the 'Select Services' tab active. The dialog has three tabs: 'Define Feed', 'Select Services', and 'Review'. Below the tabs, there are two sub-tabs: 'Services' (selected) and 'Groups'. A table lists available services:

<input type="checkbox"/>		Name ^	Address	Type
<input type="checkbox"/>		192.168.1.102 Decoder	192.168.1.102	Decoder
<input type="checkbox"/>		192.168.1.101 Log Decoder	192.168.1.101	Log Decoder

At the bottom of the dialog, there are four buttons: 'Reset', 'Cancel', 'Prev', and 'Next'. The 'Next' button is highlighted in blue.

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.



The screenshot shows the 'Configure Identity Feed' wizard with three steps: Define Feed, Select Services, and Review. The 'Define Feed' step is active. It contains a 'Feed Details' section with 'Name' set to 'Testing' and 'Feed File' set to 'zip sample.zip'. Below this is a 'Service Details' section with 'Services' set to 'Decoder'. At the bottom are buttons for 'Reset', 'Cancel', 'Prev', and 'Next'.

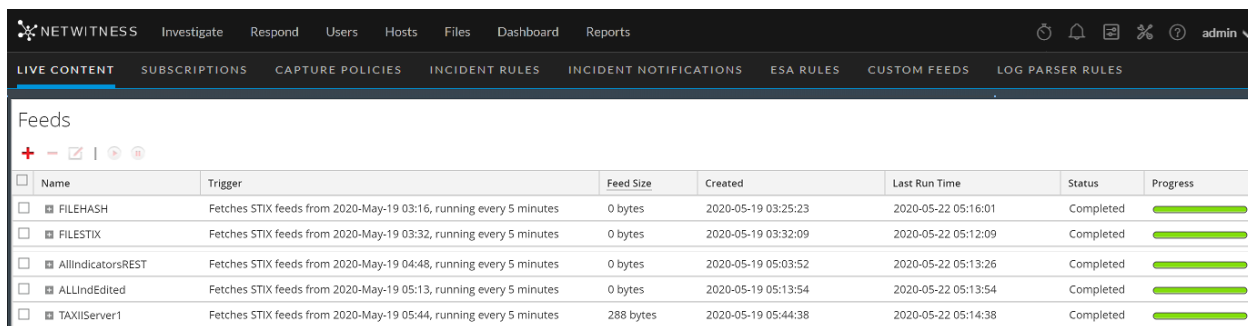
**Note:** If a group of devices with Decoders and Log Decoders is used to create recurring or custom feeds and this group is deleted, you can edit the feed and add a new group to the feed.

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.



The screenshot shows the 'Feeds' grid in the NetWitness interface. It includes a table with columns: Name, Trigger, Feed Size, Created, Last Run Time, Status, and Progress. There are five rows of feeds, all with a status of 'Completed' and a full progress bar.

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	100%
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	100%
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	100%
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	100%
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	100%



### 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 **jettysrv** 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.

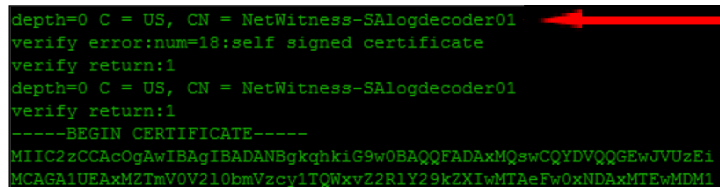
1. SSH to the NetWitness UI server.
2. Run the following command to output the CN name of the SSL cert:

```
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-----  
MIIC2zCCAcOgAwIBAgIBADANBgkqhkiG9w0BAQQFADAxMQswCQYDVQQGEwJVUzE1  
MCAGA1UEAxMZTmV0V210bmVzcy1TQWxvZ2R1Y29kZ2XiMTAeFw0xNDExMTEwMDM1
```

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.

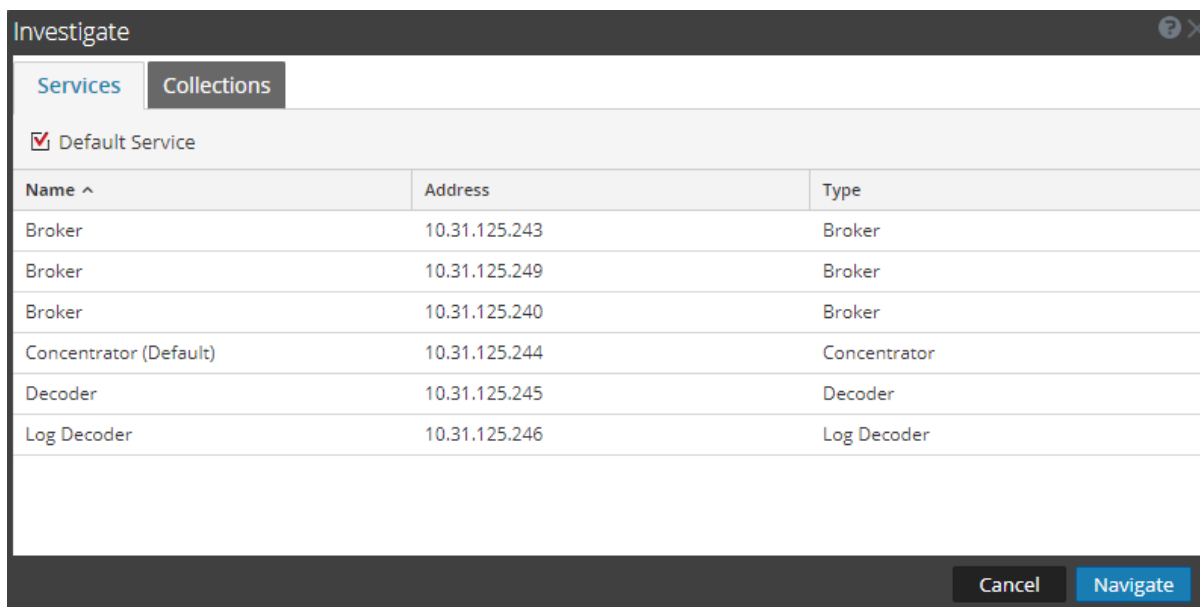
**Note:** An identity feed only tracks one log in at a time. If two users log in to a system at the same time, the second user will overwrite the first user's data in the identity feed.

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

#### To investigate a configured identity feed:

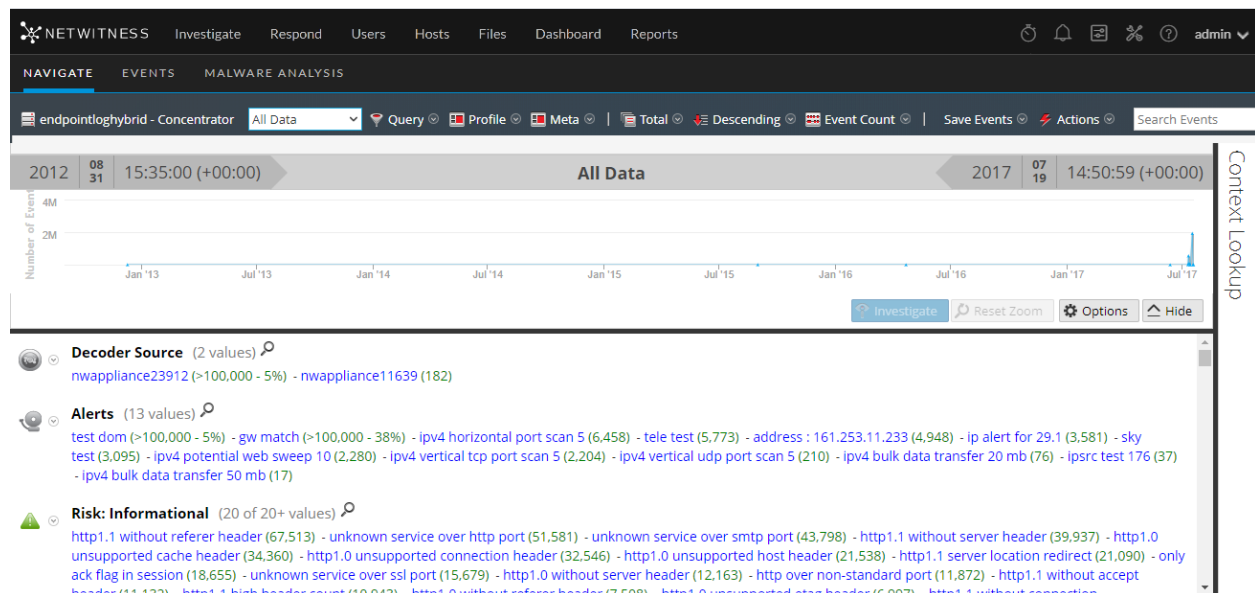
1. Go to **INVESTIGATE > Navigate**.

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.

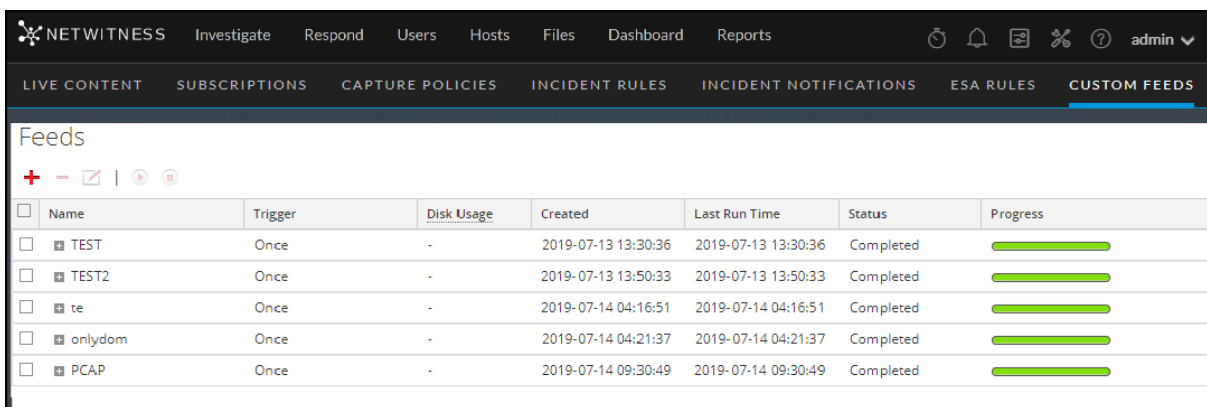
After you edit a feed:

- 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**.

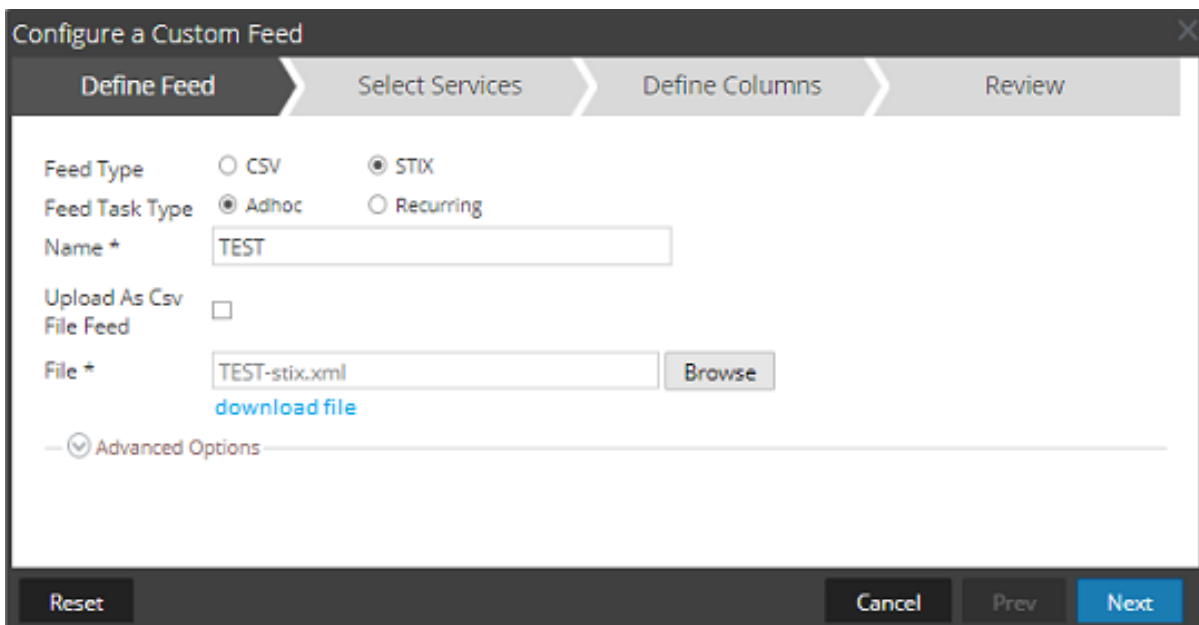
The Custom Feeds dialog is displayed.



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

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.

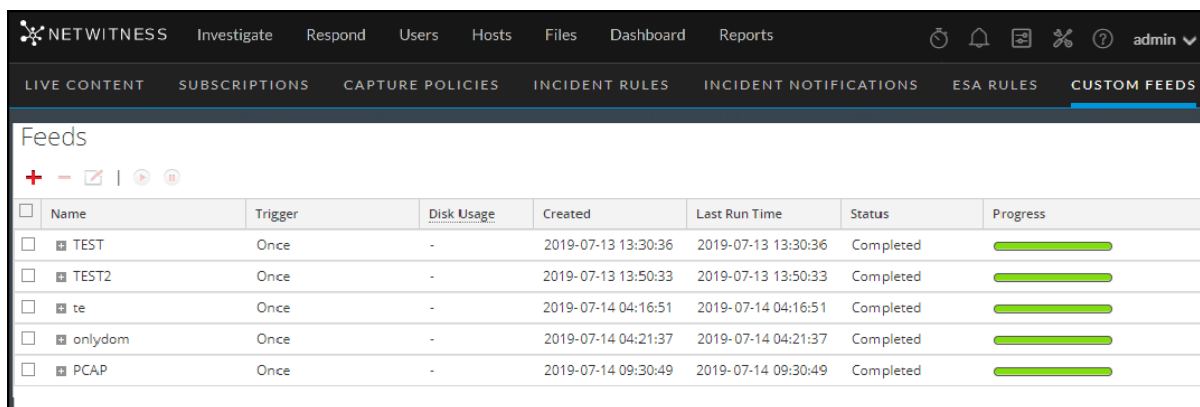
## Removing a Feed

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**.

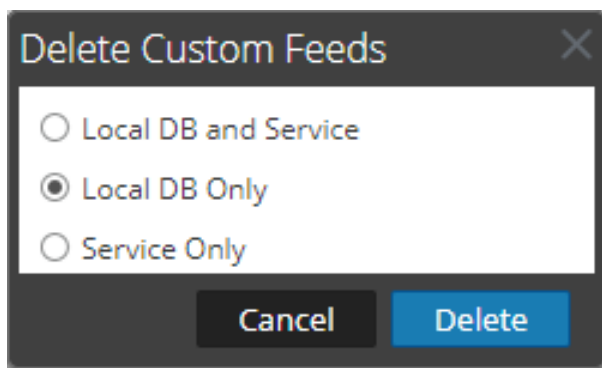
The Custom Feeds dialog is displayed.



	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></div>
<input type="checkbox"/>	TEST2	Once	-	2019-07-13 13:50:33	2019-07-13 13:50:33	Completed	<div></div>
<input type="checkbox"/>	te	Once	-	2019-07-14 04:16:51	2019-07-14 04:16:51	Completed	<div></div>
<input type="checkbox"/>	onlydom	Once	-	2019-07-14 04:21:37	2019-07-14 04:21:37	Completed	<div></div>
<input type="checkbox"/>	PCAP	Once	-	2019-07-14 09:30:49	2019-07-14 09:30:49	Completed	<div></div>

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

The Delete Custom Feeds dialog is displayed.



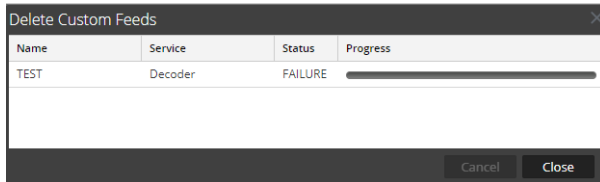
You can select one of the following options to delete the feed:

- 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 RSA 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.



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:**

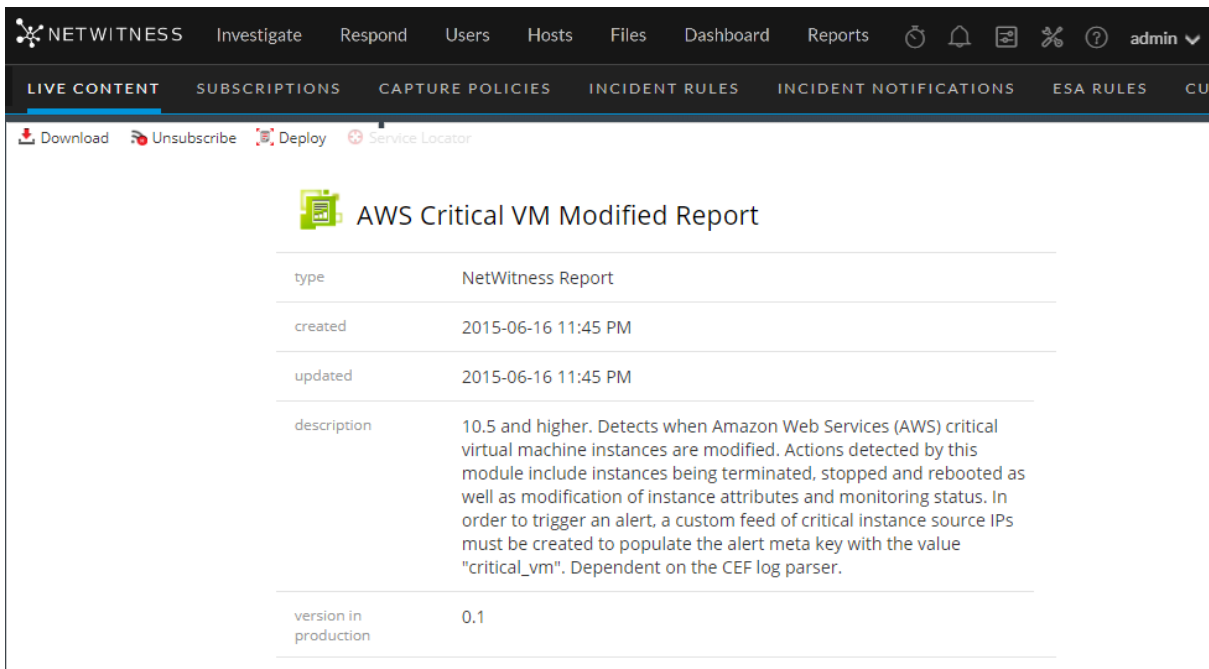
1. Go to  (Configure) > **Live Content**.
2. In the **Search Criteria** panel, specify search criteria and click **Search**.
3. Select one or more resources and click  **Subscribe**.  
A confirmation dialog is displayed: **By subscribing to these resources, you are indicating that you wish to receive 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:

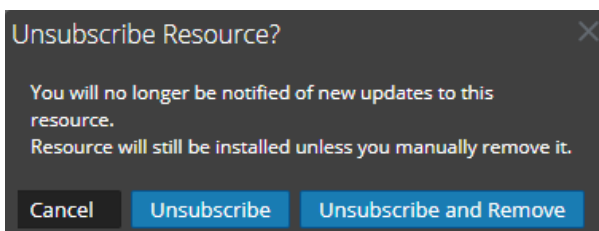
- Perform a search,  **(Configure)** > **Live Content** > enter search criteria, then select the resource in the Matching Resources panel, then click  **Details**.
- View subscriptions,  **(Configure)** > **Subscriptions**, select the resource from the Subscriptions list, then click  **Details**.



The screenshot shows the NetWitness interface with the 'LIVE CONTENT' tab selected. The resource 'AWS Critical VM Modified Report' is displayed with the following details:

type	NetWitness Report
created	2015-06-16 11:45 PM
updated	2015-06-16 11:45 PM
description	10.5 and higher. Detects when Amazon Web Services (AWS) critical virtual machine instances are modified. Actions detected by this module include instances being terminated, stopped and rebooted as well as modification of instance attributes and monitoring status. In order to trigger an alert, a custom feed of critical instance source IPs must be created to populate the alert meta key with the value "critical_vm". Dependent on the CEF log parser.
version in production	0.1

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



The dialog box titled 'Unsubscribe Resource?' contains the following text:

You will no longer be notified of new updates to this resource.  
Resource will still be installed unless you manually remove it.

At the bottom, there are three buttons: **Cancel**, **Unsubscribe**, and **Unsubscribe and Remove**.

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 **Detailed Results**, click the resource type icon or the resource name.

The screenshot displays the NetWitness Live Resource View interface. The top navigation bar includes tabs for Investigate, Respond, Users, Hosts, Files, Dashboard, and Reports. The main header shows 'LIVE CONTENT' and various subscription and policy management options. On the left, the 'Search Criteria' panel is active, showing a search for 'malware' with filters for Category (Threat, Identity, Assurance, Operations) and Resource Types (Medium). The 'Matching Resources' panel on the right lists four resources:

- Malware Domains**: type Feed, updated 2017-07-19 1:02 AM, version 0.869, size 2.11 MB, subscribed yes. List of domains associates with malware sourced from www.malwaredomains.com. Includes meta keys: threat, malware, threat.category, threat.desc, threat.source, malwaredomains.com.
- Malware Domain List**: type Feed, updated 2017-07-17 12:40 AM, version 0.1490, size 85.91 KB, subscribed no. List of domains commonly associated with malware sourced from www.malwaredomainlist.com. Includes meta keys: threat, malware, threat.category, threat.desc, threat.source, malwaredomainlist-domain.
- Malware IP List**: type Feed, updated 2017-07-17 12:45 AM, version 0.1567, size 32.55 KB, subscribed yes. List of ip addresses commonly associated with malware sourced from www.malwaredomainlist.com. Includes meta keys: threat, malware, threat.category, threat.desc, threat.source, malwaredomainlist-ip.
- Malware PDF**: type FlexParser, updated 2012-02-09 4:51 PM, version 0.1, size 17.51 KB, subscribed no. Legacy: Intended only for 9.8. For SA deployments version 10 and above, see lua parser fingerprint\_pdf\_lua. Detects PDF files that contain javascript or launch actions.

At the bottom of the Matching Resources panel, it indicates '57 Matching Resources'.

- If you are viewing the list results, double-click a resource or select a resource and click **Details**.

The screenshot shows the NETWITNESS interface with the following components:

- Top Navigation Bar:** Includes icons for Investigate, Respond, Users, Hosts, Files, Dashboard, and Reports. On the right, there are icons for a clock, a bell, a list, a magnifying glass, and a user profile labeled 'admin'.
- Sub Navigation Bar:** Includes links for LIVE CONTENT, SUBSCRIPTIONS, CAPTURE POLICIES, INCIDENT RULES, INCIDENT NOTIFICATIONS, ESA RULES, CUSTOM FEEDS, and LOG PARSER RULES.
- Search Criteria Panel (Left):**
  - Keywords:** A text input field containing 'malware'.
  - Category:** A list of categories with checkboxes: FEATURED, THREAT, IDENTITY, ASSURANCE, and OPERATIONS.
  - Resource Types:** A dropdown menu.
  - Medium:** A dropdown menu.
  - Required Meta Keys:** A text input field.
  - Generated Meta Values:** A text input field.
  - Search Button:** A blue button labeled 'Search'.
- Matching Resources Table (Right):**
  - Actions:** Show Results, Details, Deploy, Subscribe, Package.
  - Table Headers:** Subscribed, Name, Created, Updated, Type, Description.
  - Table Rows:**
    - ☒ yes **Malware Domains** 2012-02-09 4:48 PM 2017-07-21 1:02 AM Feed List of domains associ
    - ☐ yes Malware IP List 2012-02-09 4:48 PM 2017-07-20 7:21 PM Feed List of ip addresses con
    - ☐ no Malware Domain List 2012-02-09 4:48 PM 2017-07-20 7:30 PM Feed List of domains commo
    - ☐ yes Malware PDF 2012-02-09 4:51 PM 2012-02-09 4:51 PM FlexParser Legacy: Intended only fi
    - ☐ no Malware Activity Report 2017-03-14 3:21 PM 2017-03-14 3:21 PM NetWitness Report Displays traffic that has
    - ☐ no Malware Activity DNS 2017-03-14 3:18 PM 2017-03-14 3:18 PM NetWitness Rule Displays DNS packet tra
    - ☐ no Malware Activity Unidentified 2017-03-14 3:18 PM 2017-03-14 3:18 PM NetWitness Rule Displays packet and log
    - ☐ no Malware Activity Web 2017-03-14 3:18 PM 2017-03-14 3:18 PM NetWitness Rule Displays web-based pac
    - ☐ no SchoolBell Malware 2016-10-25 6:05 PM 2016-10-25 6:05 PM Application Rule The SchoolBell rule dete
    - ☐ no Flame Malware Detection 2012-05-31 8:18 PM 2012-06-05 2:35 PM FlexParser Legacy: Intended only fi
    - ☐ no RSA FirstWatch Command ... 2012-12-23 12:36 AM 2017-07-20 7:20 PM Feed This feed contains IPs tl
    - ☐ no RSA FirstWatch Command ... 2012-12-23 12:36 AM 2017-07-20 7:20 PM Feed This feed contains Dom
    - ☐ no Dreambot Malware 2017-04-04 7:36 PM 2017-04-04 7:36 PM Application Rule The Dreambot is a bank
    - ☐ no Mirage Malware 2016-08-09 6:27 PM 2016-08-09 6:27 PM Application Rule Detects malicious outb

## 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.

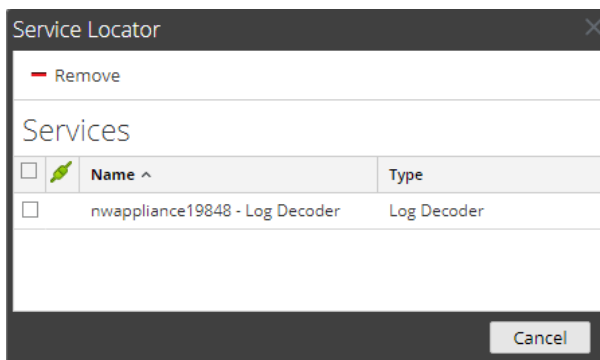
## Locating and Removing a Deployed Resource from Services

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.

**Search Criteria**

Keywords:

Category:

- ☐ FEATURED
- ☒ THREAT
- ☐ IDENTITY
- ☐ ASSURANCE
- ☐ OPERATIONS

Resource Types:

Medium:

Required Meta Keys:

Generated Meta Values:

**Search**

**Matching Resources**

☐ Show Results | 
 ☐ Details | 
 ☒ Deploy | 
 ☐ Subscribe | 
 ☒ Package

<input type="checkbox"/>	Subscribed	Name	Created	Updated	Type	Description
<input checked="" type="checkbox"/>	yes	Malware Domains	2012-02-09 4:48 PM	2017-07-21 1:02 AM	Feed	List of domains associ
<input type="checkbox"/>	yes	Malware IP List	2012-02-09 4:48 PM	2017-07-20 7:21 PM	Feed	List of ip addresses con
<input type="checkbox"/>	no	Malware Domain List	2012-02-09 4:48 PM	2017-07-20 7:30 PM	Feed	List of domains commo
<input type="checkbox"/>	yes	Malware PDF	2012-02-09 4:51 PM	2012-02-09 4:51 PM	FlexParser	Legacy: Intended only fi
<input type="checkbox"/>	no	Malware Activity Report	2017-03-14 3:21 PM	2017-03-14 3:21 PM	NetWitness Report	Displays traffic that has
<input type="checkbox"/>	no	Malware Activity DNS	2017-03-14 3:18 PM	2017-03-14 3:18 PM	NetWitness Rule	Displays DNS packet tre
<input type="checkbox"/>	no	Malware Activity Unidentified	2017-03-14 3:18 PM	2017-03-14 3:18 PM	NetWitness Rule	Displays packet and log
<input type="checkbox"/>	no	Malware Activity Web	2017-03-14 3:18 PM	2017-03-14 3:18 PM	NetWitness Rule	Displays web-based pac
<input type="checkbox"/>	no	SchoolBell Malware	2016-10-25 6:05 PM	2016-10-25 6:05 PM	Application Rule	The SchoolBell rule dete
<input type="checkbox"/>	no	Flame Malware Detection	2012-05-31 8:18 PM	2012-06-05 2:35 PM	FlexParser	Legacy: Intended only fi
<input type="checkbox"/>	no	RSA FirstWatch Command ...	2012-12-23 12:36 AM	2017-07-20 7:20 PM	Feed	This feed contains IPs tl
<input type="checkbox"/>	no	RSA FirstWatch Command ...	2012-12-23 12:36 AM	2017-07-20 7:20 PM	Feed	This feed contains Dom
<input type="checkbox"/>	no	Dreambot Malware	2017-04-04 7:36 PM	2017-04-04 7:36 PM	Application Rule	The Dreambot is a bank
<input type="checkbox"/>	no	Mirage Malware	2016-08-09 6:27 PM	2016-08-09 6:27 PM	Application Rule	Detects malicious outbc

57 Matching Resources

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

The screenshot shows the NetWitness Live Content interface. The top navigation bar includes tabs for Investigate, Respond, Users, Hosts, Files, Dashboard, and Reports. Below this is a secondary navigation bar with tabs for LIVE CONTENT, SUBSCRIPTIONS, CAPTURE 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 fields for Keywords (with 'malware' entered), Category (with a tree view showing FEATURED, THREAT, IDENTITY, ASSURANCE, and OPERATIONS), Resource Types (a dropdown menu), Medium (a dropdown menu), Required Meta Keys (a text field), and Generated Meta Values (a text field). A 'Search' button is at the bottom of this panel. The right panel, titled 'Matching Resources', displays a list of resources. At the top of this panel are icons for Show Results, Details, Deploy, Subscribe, and Package. The list includes:
 


- Malware Domains**: type Feed, updated 2017-07-19 1:02 AM, version 0.869, size 2.11 MB, subscribed yes. Description: List of domains associates with malware sourced from www.malwaredomains.com. Tags: threat, malware, threat.category, threat.desc, threat.source, malwaredomains.com.
- Malware Domain List**: type Feed, updated 2017-07-17 12:40 AM, version 0.1490, size 85.91 KB, subscribed no. Description: List of domains commonly associated with malware sourced from www.malwaredomainlist.com. Tags: threat, malware, threat.category, threat.desc, threat.source, malwaredomainlist-domain.
- Malware IP List**: type Feed, updated 2017-07-17 12:45 AM, version 0.1567, size 32.55 KB, subscribed yes. Description: List of ip addresses commonly associated with malware sourced from www.malwaredomainlist.com. Tags: threat, malware, threat.category, threat.desc, threat.source, malwaredomainlist-ip.
- Malware PDF**: type FlexParser, updated 2012-02-09 4:51 PM, version 0.1, size 17.51 KB, subscribed no. Description: Legacy: Intended only for 9.8. For SA deployments version 10 and above, see lua parser fingerprint\_pdf\_lua Detects PDF files that contain javascript or launch actions.

 At the bottom of the right panel, it says '57 Matching Resources'.

### Viewing Resource Details

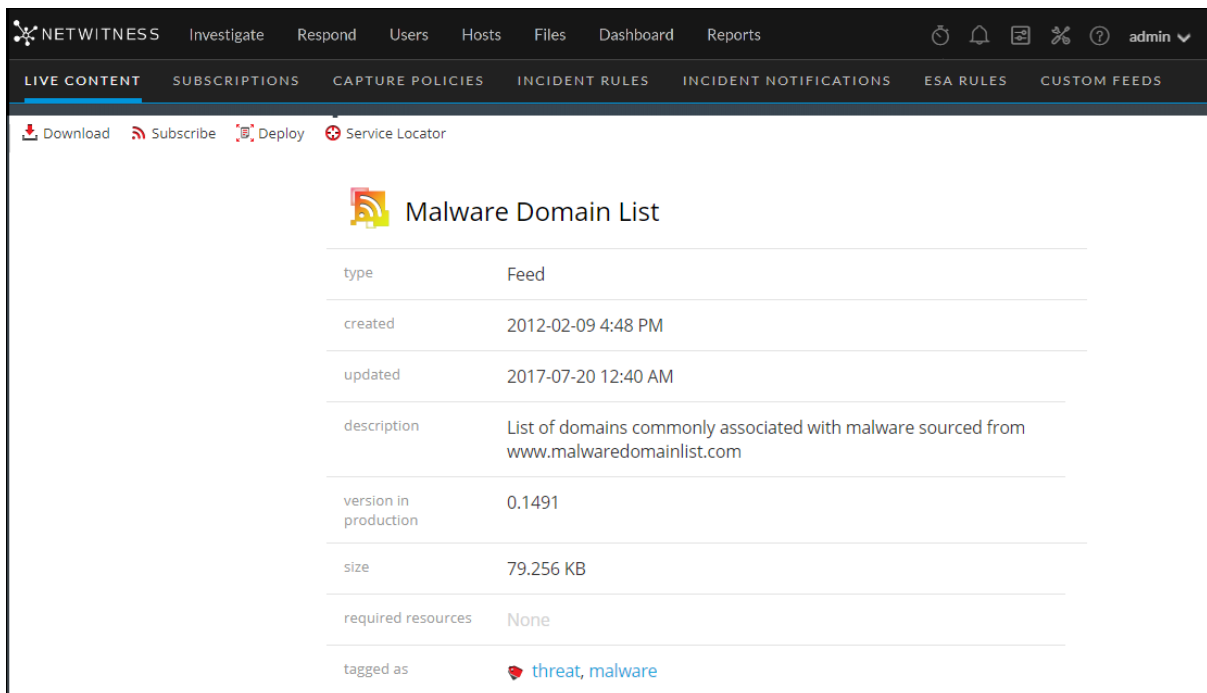
You can display detailed information about a subscribed resource in the Resource View.

#### 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 shows the NetWitness Live Content interface. The top navigation bar includes 'NETWITNESS' and various menu items: Investigate, Respond, Users, Hosts, Files, Dashboard, and Reports. On the right, there are icons for a clock, a bell, a document, a percentage, a question mark, and a user profile labeled 'admin'. Below the navigation bar, a secondary bar contains 'LIVE CONTENT' (highlighted), SUBSCRIPTIONS, CAPTURE POLICIES, INCIDENT RULES, INCIDENT NOTIFICATIONS, ESA RULES, and CUSTOM FEEDS. Under 'LIVE CONTENT', there are four action buttons: Download, Subscribe, Deploy, and Service Locator. The main content area displays the details for a resource titled 'Malware Domain List', which is represented by a feed icon. The details are organized into a table-like structure with the following rows:

type	Feed
created	2012-02-09 4:48 PM
updated	2017-07-20 12:40 AM
description	List of domains commonly associated with malware sourced from <a href="http://www.malwaredomainlist.com">www.malwaredomainlist.com</a>
version in production	0.1491
size	79.256 KB
required resources	None
tagged as	 threat, malware

## 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

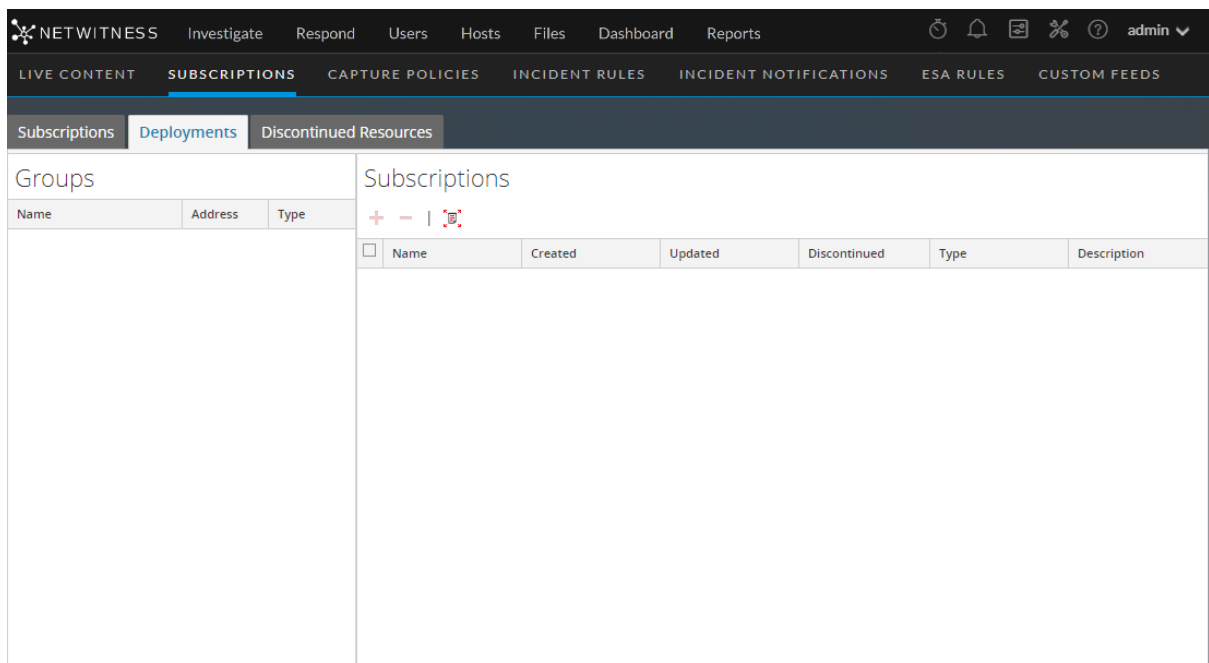
synchronize immediately in the  **(Configure) > Subscriptions > Deployments** tab.

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.
<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 RSA 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.

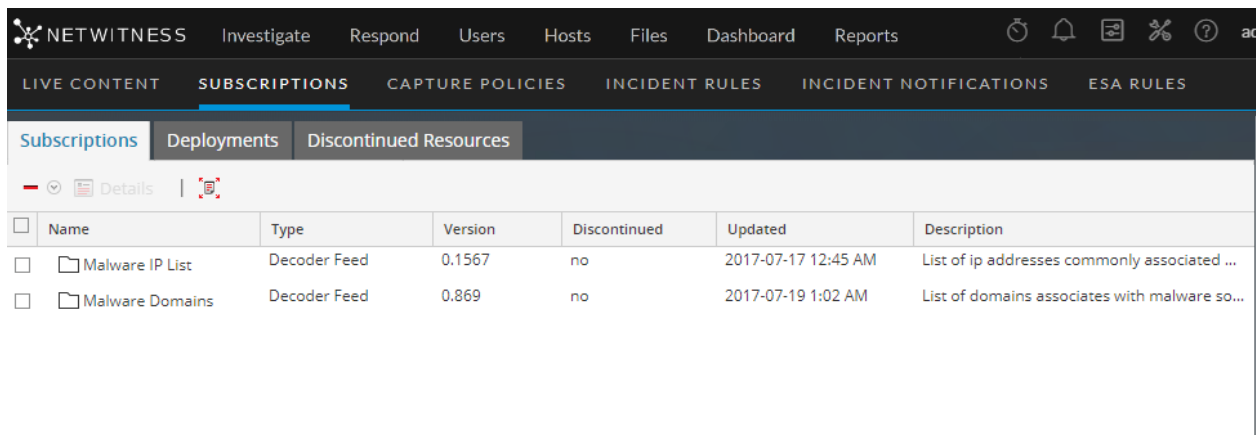
In the Subscriptions tab, you can:



- 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.
 <b>Details</b>	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**.

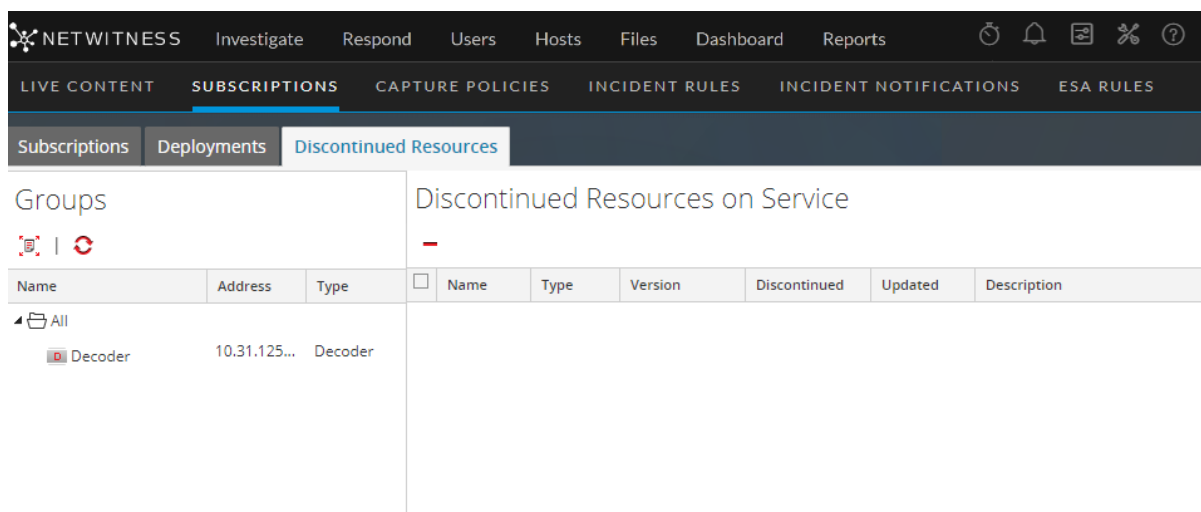
### To access this view:

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

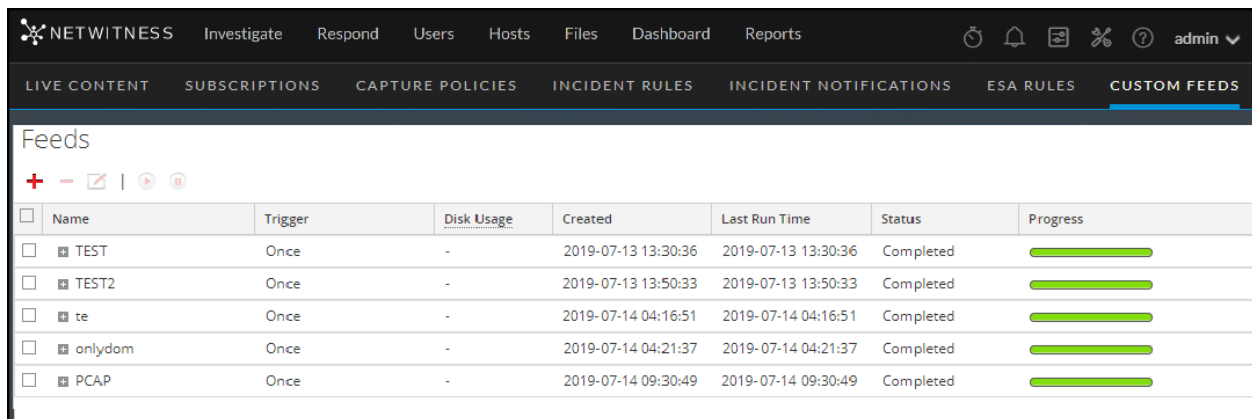
Use the Live Feeds View to:

- 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.


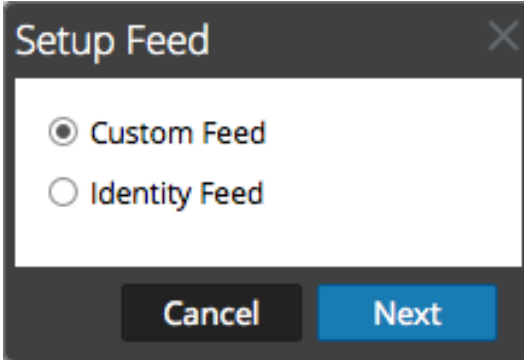






	Name	Trigger	Disk Usage	Created	Last Run Time	Status	Progress
<input type="checkbox"/>	TEST	Once	-	2019-07-13 13:30:36	2019-07-13 13:30:36	Completed	<div></div>
<input type="checkbox"/>	TEST2	Once	-	2019-07-13 13:50:33	2019-07-13 13:50:33	Completed	<div></div>
<input type="checkbox"/>	te	Once	-	2019-07-14 04:16:51	2019-07-14 04:16:51	Completed	<div></div>
<input type="checkbox"/>	onlydom	Once	-	2019-07-14 04:21:37	2019-07-14 04:21:37	Completed	<div></div>
<input type="checkbox"/>	PCAP	Once	-	2019-07-14 09:30:49	2019-07-14 09:30:49	Completed	<div></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> <b>Note:</b> You can now use special characters to define the name of the custom feed. </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:

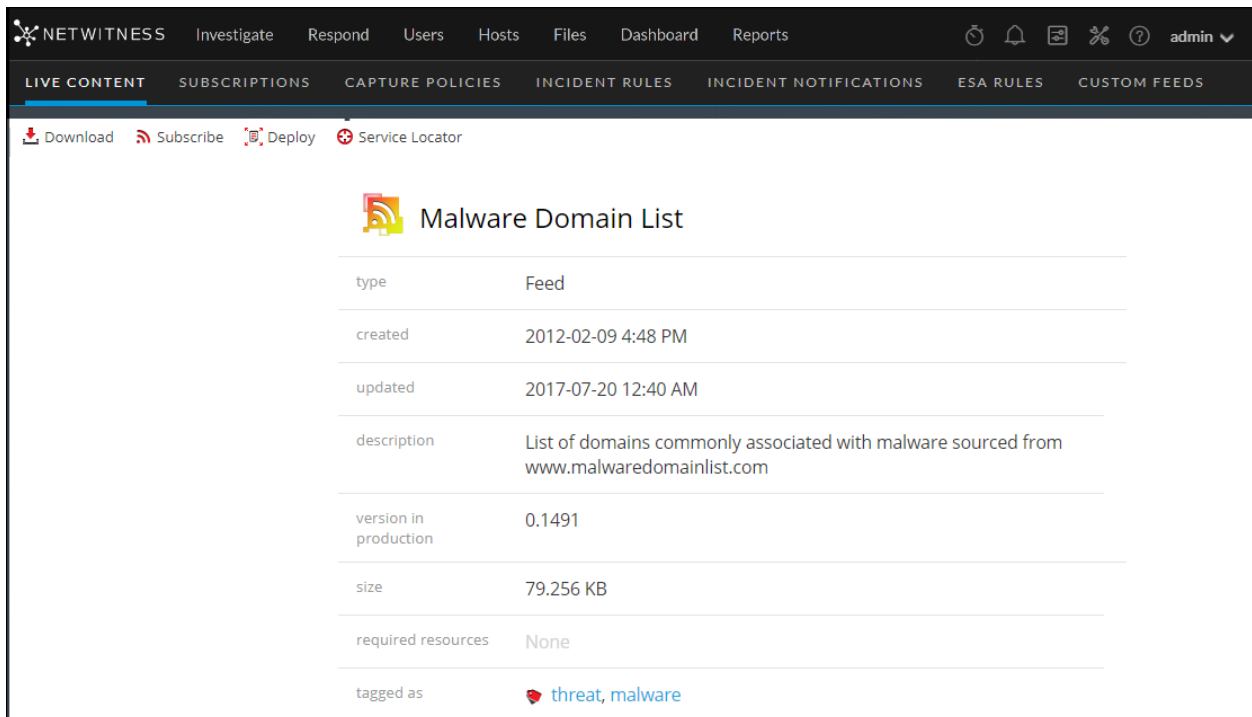
- Download the resource.
- Subscribe or unsubscribe the resource.
- Deploy the resource to services.
- Locate services on which the resource is deployed and remove the resource from services.

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 interface with the 'LIVE CONTENT' tab selected. Below the navigation bar, there are icons for Download, Subscribe, Deploy, and Service Locator. The main content area displays details for a resource named 'Malware Domain List'.

type	Feed
created	2012-02-09 4:48 PM
updated	2017-07-20 12:40 AM
description	List of domains commonly associated with malware sourced from <a href="http://www.malwaredomainlist.com">www.malwaredomainlist.com</a>
version in production	0.1491
size	79.256 KB
required resources	None
tagged as	 threat, malware

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


## Resource Details

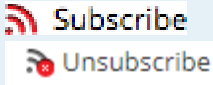

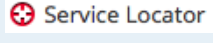
The following table describes the elements in the Resource Details section.

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</b> , <b>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>	 The icon shows two buttons: 'Subscribe' with a red RSS-like signal icon and 'Unsubscribe' with a red RSS-like signal icon and a red 'x'.	<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>	 The icon shows a button with a red square icon containing a white 'D' and the text 'Deploy'.	<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>	 The icon shows a button with a red circle icon containing a white cross and the text 'Service Locator'.	<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 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.

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.
<b>Resource Types</b>	<p>Select resource 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> <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>



Feature	Description
<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>
<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> . <b>Note:</b> (Discontinued) is displayed next to the resource name if a resource is discontinued.
<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> .
<b>Size</b>	The size of the resource, for example, <b>153 B</b> .
<b>Subscribed</b>	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>
<b>Description</b>	The description of the resource, for example, <b>Compliance Rule-Group Management</b> .
<b>Tags</b>	The tags that apply to the resource. Clicking a tag narrows the search to resources with that tag. For example,  .
<b>Meta Keys</b>	The meta keys that apply to the resource. Clicking a meta key narrows the search to resources with that meta key. For example,  .
<b>Resource Meta Values</b>	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
<b>Subscribed</b>	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>
<b>Name</b>	The name of the resource, for example, <b>Group Management</b> . <b>Note:</b> The resource name is displayed in red color if it is discontinued.
<b>Created</b>	The date when the resource was created, for example, <b>2015-08-12 3:11 PM</b> .
<b>Updated</b>	The date when the resource was last updated, for example, <b>2015-09-15 4:27 PM</b> .

Feature	Description
Type	The type of the resource, for example, <b>Rule</b> .
Discontinued	<p>The status of the discontinued resources:</p> <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	
 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	<p>This menu offers two packaging functions for the selected resources:</p> <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 ( Deploy), see [Find and Deploy Live Resources](#).
- For more information on Deploying a Package ( 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.

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

Showing **New Content (12)** Timezone: GMT+0530 Asia/Calcutta

NAME	CREATED	UPDATED	TYPE	MIN PLATFORM VERSION	DESCRIPTION
Microsoft Document Spa...	07-Sep-2022 18:...	07-Sep-2022 18:...	Application Rule	11.5	Detects a Windows command and scripting interpreter exe...
UAC Bypass via COM Obj...	30-Aug-2022 18:...	30-Aug-2022 23:...	Application Rule	11.5	Identifies User Account Control (UAC) bypass attempts usi...
O365 - Multiple Failed Lo...	26-Aug-2022 19:...	26-Aug-2022 19:...	Event Stream An...	11.5	When attempting to access O365 environments, actors ma...
Quasar RAT Default Persi...	25-Aug-2022 22:...	25-Aug-2022 22:...	Application Rule	All Versions	In environments where admin privileges have already been...
Quasar RAT Default SSL ...	25-Aug-2022 22:...	25-Aug-2022 22:...	Application Rule	All Versions	C2 communication for Quasar RAT uses a common SSL Cer...
Outbound Network Conn...	25-Aug-2022 16:...	25-Aug-2022 16:...	Application Rule	All Versions	This rule helps to detect regsvr32.exe, rundll32.exe, and dll...
Unexpected fodhelper.ex...	25-Aug-2022 16:...	25-Aug-2022 16:...	Application Rule	All Versions	fodhelper (Features On Demand Helper) is an executable u...
Raspberry Robin C2 Com...	25-Aug-2022 16:...	25-Aug-2022 16:...	Application Rule	All Versions	Raspberry Robin, the LNK Worm, is commonly known to d...
cmd.exe Reads and Execu...	25-Aug-2022 16:...	25-Aug-2022 16:...	Application Rule	All Versions	Adversaries can use the command prompt feature cmd/R <...
WhisperGate - Advanced...	19-Aug-2022 22:...	19-Aug-2022 22:...	Application Rule	All Versions	WhisperGate, a type of data wiping malware, is commonl...
WhisperGate - Self Remo...	19-Aug-2022 22:...	19-Aug-2022 22:...	Application Rule	All Versions	Towards it's final execution steps, WhisperGate, the data w...
WhisperGate - Powershel...	19-Aug-2022 22:...	19-Aug-2022 22:...	Application Rule	All Versions	WhisperGate, a type of data wiping malware, is commonl...

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

Showing **Filtered Content (2)** Timezone: GMT+0530 Asia/Calcutta

NAME	CREATED	UPDATED	TYPE	MIN PLATFORM VERSION	DESCRIPTION
[Community] Possible Sus...	19-Aug-2022 22:...	19-Aug-2022 22:...	Application Rule	NA	Data Wiping Malwares may partially or completely overwr...
[Community] Potential M...	18-Aug-2022 21:...	18-Aug-2022 21:...	Application Rule	NA	Detects a successful ProxyShell exploitation attack (CVE-2...

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 in-built content that NetWitness Platform Live provides.
<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 screenshot shows a dark-themed search interface. At the top, there's a 'SOURCE' dropdown set to 'Community'. Below it is an 'Only Opensource' checkbox. The 'Content' section has a blue plus icon. The 'Search Content' section also has a blue plus icon. Below these are several filter sections: 'KEYWORDS' with a text input, 'RESOURCE TYPES' with a 'Please select' dropdown, 'MEDIUMS' with a 'Please select' dropdown, 'TAGS' with a 'PRW X' button and a dropdown, 'PLATFORM VERSIONS' with a '11.5.0.0 X' button and a dropdown, 'REQUIRED META KEYS' with a text input, and 'GENERATED META VALUES' with a text input. At the bottom, there are date range pickers for 'CREATED DATE' (2022-08-16 to 2022-09-06) and 'MODIFIED DATE' (Start date to End date). There's also a checked checkbox for 'Include Discontinued'. At the very bottom are 'Search' and 'Reset Filter' buttons.

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 later): 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.

Content						
View New, recently updated and community content details here.						
Showing <b>Filtered Content (877)</b>				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 I...</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

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>

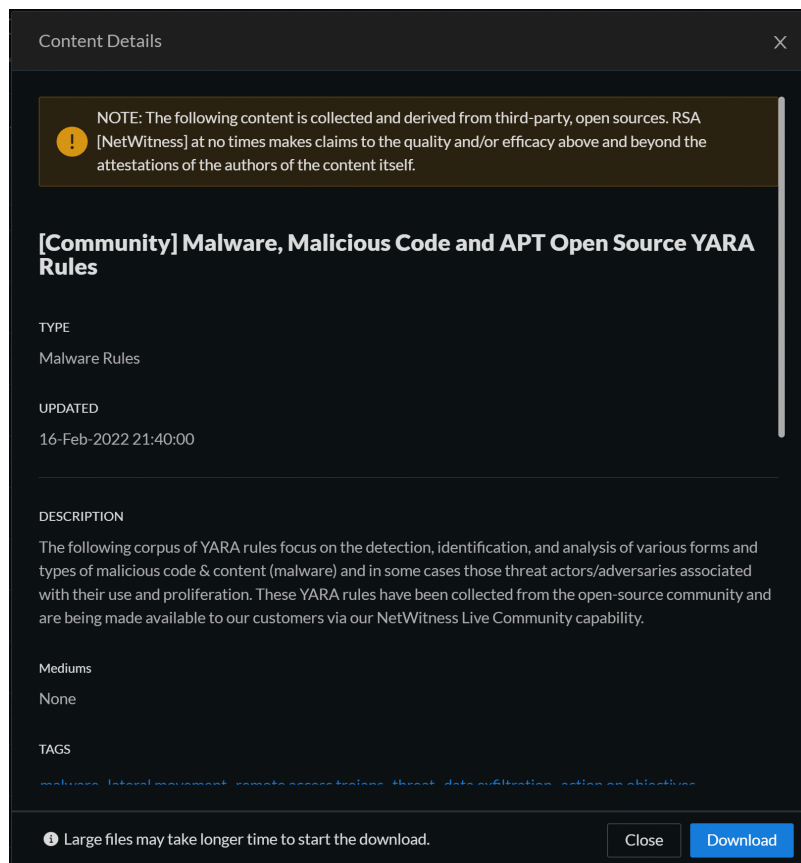
### Content Details Panel

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 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>• <b>Yes:</b> The content that matches the search criteria is discontinued</li><li>• <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.

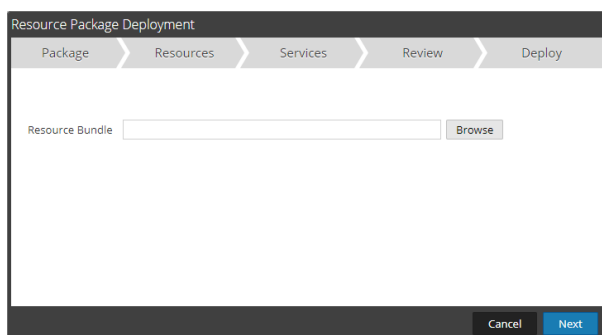
**Note:** Use NetWitness Live to create resource bundles; this is a different application that is not part of NetWitness. Selecting **Package > Create** in the **Live Search - Matching Resources** toolbar displays the Content Package Tool window. You can choose resources to include in a package and save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

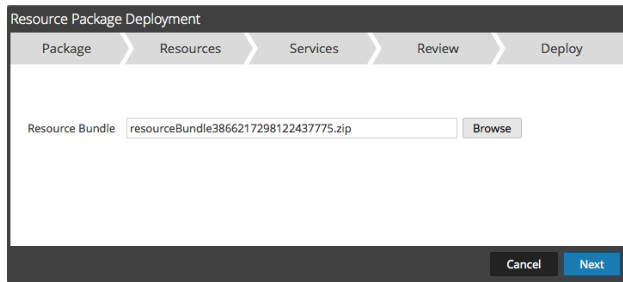
The Deployment Wizard has five tabs: **Package**, **Resources**, **Services**, **Review** and **Deploy**. Use **Close** to exit before you complete the wizard.

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

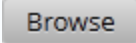
### Package Tab

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.



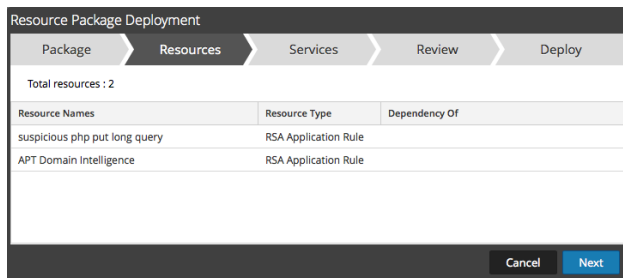
The following table describes the elements in the Package tab.

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.
<b>Command Buttons</b>	
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.

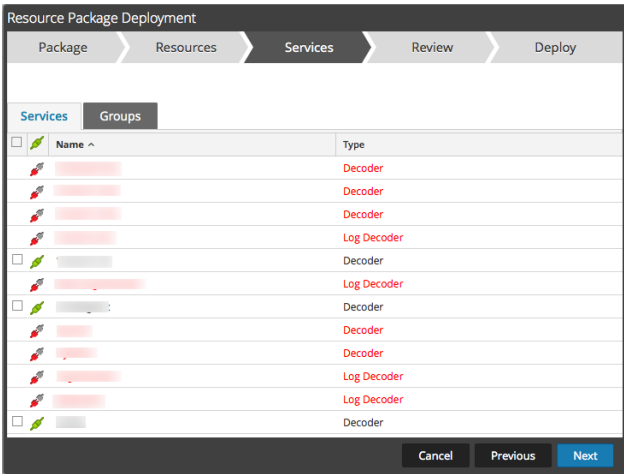
Column	Description
Resource Name	Displays the name of the resources in the bundle (for example, <b>NetWitness Lua Library</b> ).
Resource Type	Displays the resource types for the resources in the bundle (for example, <b>RSA Lua Parser</b> )
Dependency Of	Displays Resources on which the selected resource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

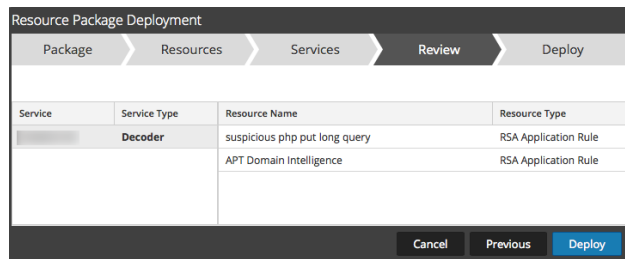
**Review Tab**

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.

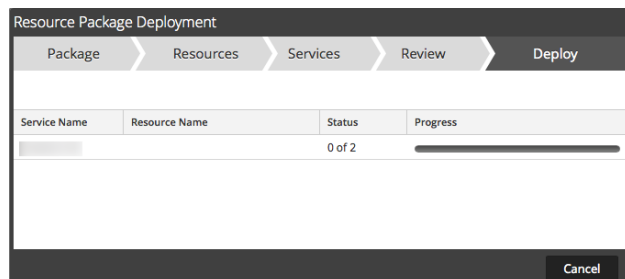
Column	Description
<b>Service Information</b>	
Service	Displays the services in your environment on which you can deploy the content.
Service Type	Displays the type of each NetWitness service (type of host or service).
<b>Resource Information</b>	
Resource Name	Displays the name of the resources you 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>.

**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**

**NETWITNESS**  
XDR Cloud Services

**Sign Up for NetWitness Live Account**

**First Name**  
Only Alphabetic, Length (3,16)

**Last Name**  
Only Alphabetic, 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 Systems Administration Page

**Username**  
Alphanumeric with \_ and -, Start with Alpha, Length (4,16)

**Password**  
Number,lower,UPPER,~,@#\$%^&\*()-+=,/,Length(8,24)

[Back to Sign In](#) **CREATE ACCOUNT**

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 <b>(missing or bad snippet) &gt; System &gt; Info</b> page.</p> <div><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.</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 **(missing or bad snippet) > 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 the 'System Logging' settings page. On the left is a navigation menu with options: 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 shows folders for 'Investigation', 'list', 'live', 'liveconnect', 'service (DEBUG)' (selected), and 'malware'. Under 'service (DEBUG)', there are four sub-items: 'LiveConnectClient', 'LiveConnectLogAggregatorService', 'LiveConnectLogParserService', and 'LiveConnectLogRetrievalService'. Below the tree view, there are input fields for 'Package' (containing 'com.rsa.smc.sa.liveconnect.service') and 'Log Level' (set to 'DEBUG' with a dropdown arrow). There is also a checkbox for 'Reset recursively' which is unchecked. At the bottom of this section are 'Apply' and 'Reset' buttons. The footer of the interface shows 'admin' as the user, 'English (United States)' as the language, and 'GMT+00:00' as the time zone.

System Logging

Realtime Historical **Settings**

Package Configuration

- Investigation
- list
- live
- liveconnect
- service (DEBUG)**
  - LiveConnectClient
  - LiveConnectLogAggregatorService
  - LiveConnectLogParserService
  - LiveConnectLogRetrievalService
- malware

Package:

Log Level:

☐ Reset recursively

**Apply** **Reset**

admin | English (United States) | 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](#)
- [About Content Library](#)
  - [Migrate Content from Core Services to Content Library](#)
  - [Import Content to Content Library](#)
  - [Create an 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](#)
- [About Groups](#)
  - [Create a Group](#)
  - [View a Group](#)
  - [Delete a Group](#)
  - [Edit a Group](#)
- [About 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](#)
- [References](#)

- [Content Library Tab](#)
- [Groups Tab](#)
- [Policies Tab](#)



## About Policy-based Centralized Content Management

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.

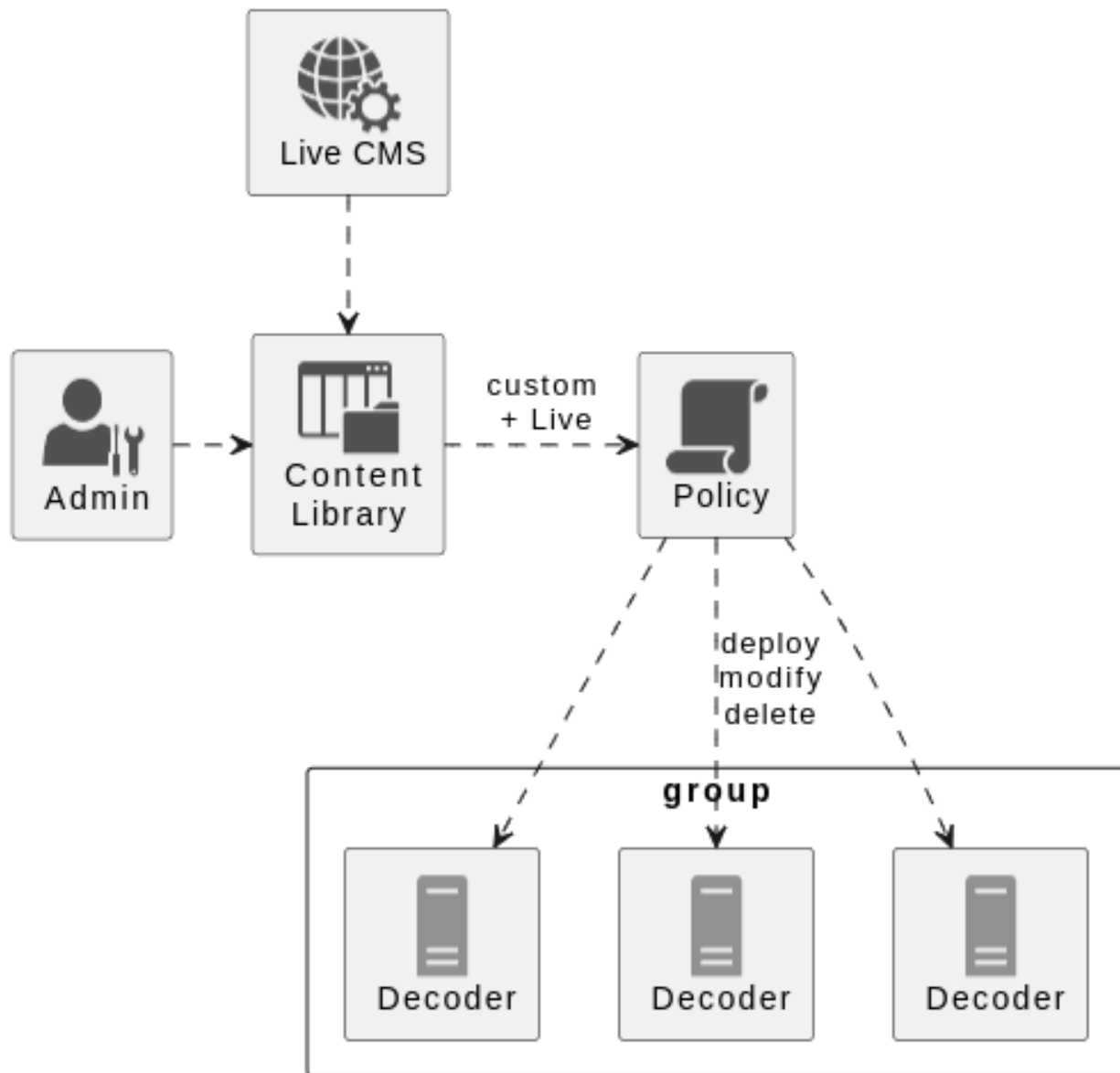
Policy-based Centralized Content Management is a unified approach to find, deploy, and manage content through the entire life cycle based on policies that can be assigned to groups of devices. It is a single location to view, modify and manage the content deployed across all services in the environment.

This approach consists of three elements:

- **Groups:** A collection of NetWitness services (such as Decoders, Log Decoders, 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.

### Content Policy Flow Diagram



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.

**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.

## 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.

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	<b>.NWR</b>	NA
Network Rules	<b>.NWR</b>	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	<b>.zip</b>	<b>.feed</b> and <b>.token</b>
Log Devices	<b>.envision</b>	NA
LUA Parsers	<b>.zip</b>	<b>.luax</b> , <b>.lua</b> and <b>.flextoken</b>

**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.

## About Content Library

This section contains:


- [Migrate Content from Core Services to Content Library](#)
- [Import Content to Content Library](#)
- [Create an 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](#)

## 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 condition for the rule.
  - Select the medium to be applied 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.

## 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 condition for the rule.
- Note:** The medium is selected as **Packet** by default, and it cannot be modified.
- 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.

### 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.

## About Groups


This section contains:

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

### 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.

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.

## 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 confirmation message is displayed.

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

**Note:** All the content within a service will be deleted when a service is removed from a group.

### About Policies


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](#)

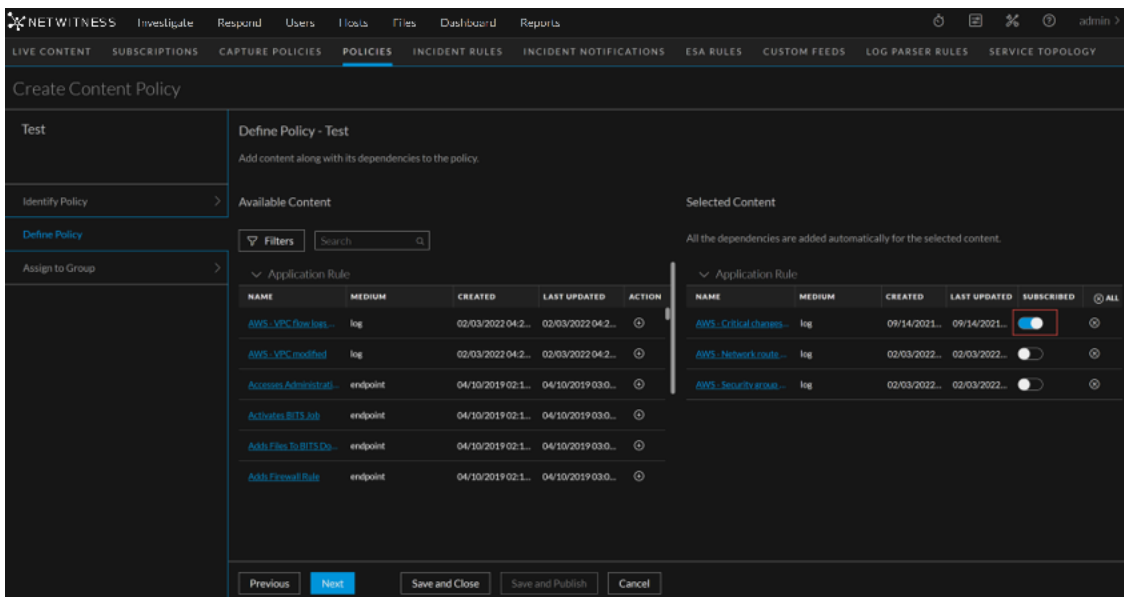
## Create and Publish Policies

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.



**Create Content Policy**

Test

Define Policy - Test

Add content along with its dependencies to the policy.

Identify Policy

Available Content

Selected Content

All the dependencies are added automatically for the selected content.

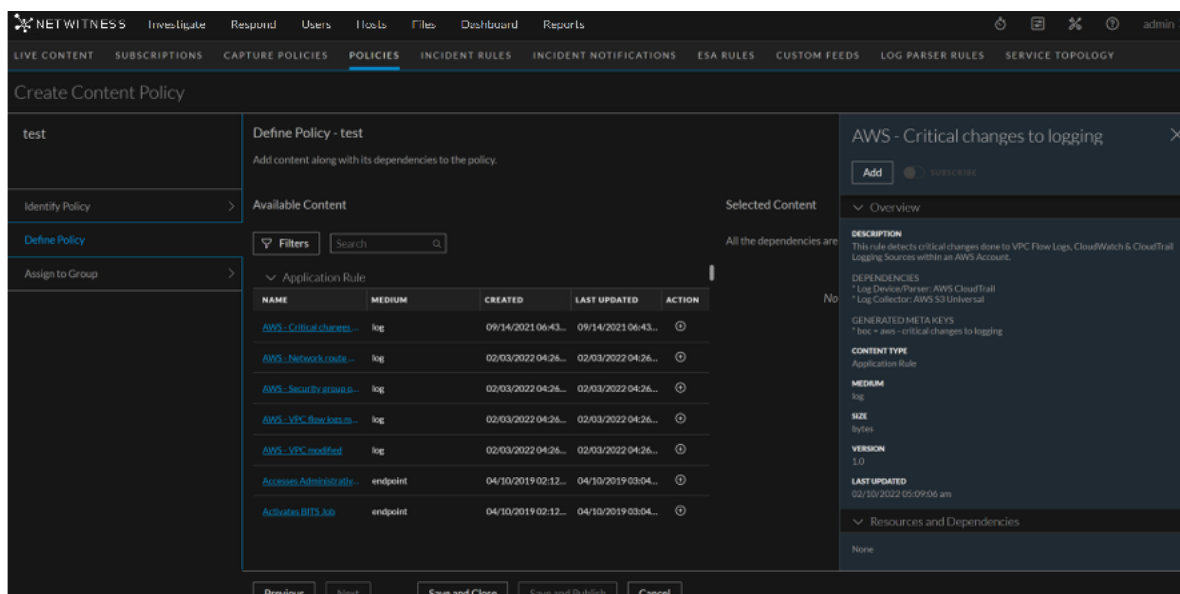
NAME	MEDIUM	CREATED	LAST UPDATED	ACTION
AWS_VPC.flowlogs...	log	02/03/2022 04:2...	02/03/2022 04:2...	⊕
AWS_VPC.modified	log	02/03/2022 04:2...	02/03/2022 04:2...	⊕
Accesses Administrative...	endpoint	04/10/2019 02:1...	04/10/2019 03:0...	⊕
Activates BITS Job	endpoint	04/10/2019 02:1...	04/10/2019 03:0...	⊕
Adds Files To BITS De...	endpoint	04/10/2019 02:1...	04/10/2019 03:0...	⊕
Adds Firewall Rule	endpoint	04/10/2019 02:1...	04/10/2019 03:0...	⊕

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"/>	⊕

Previous Next Save and Close Save and Publish Cancel

**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.



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. 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**.

**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.

- Click **Save and Close** to save the settings.

**Note:** 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.


### 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 dialog is displayed.
5. 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.

### 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.
  - 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, refer [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.
4. Click a row to view details about the selected policy.
5. 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.
6. 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.

7. To edit the policy, click **Edit Policy**. For more information on editing a policy, refer **Edit a Policy** feature.
8. To delete the policy, click **Delete Policy**. For more information on deleting a policy, refer **Delete a Policy** feature.
9. To publish the policy, click **Publish Policy**. For more information on creating and publishing a policy, refer **Create Policies** feature.
10. 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**.

## 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.

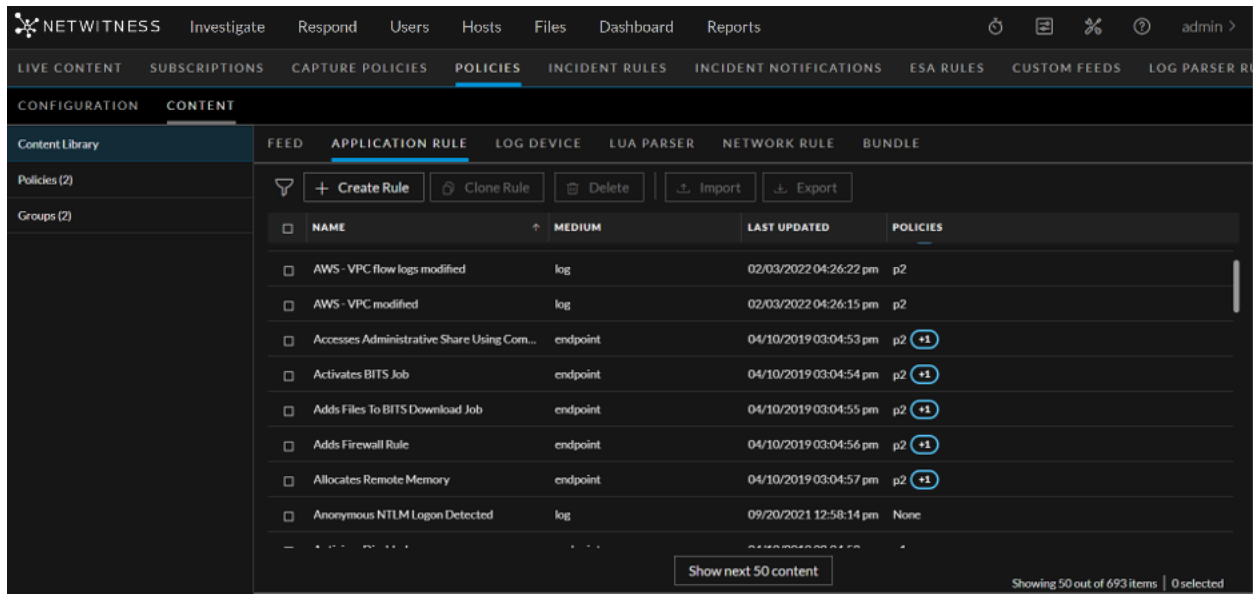
## Content Library Tab

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:




### 1 Toolbar

- Create Rule - Lets you create a rule.

### 2 Rule List Pane

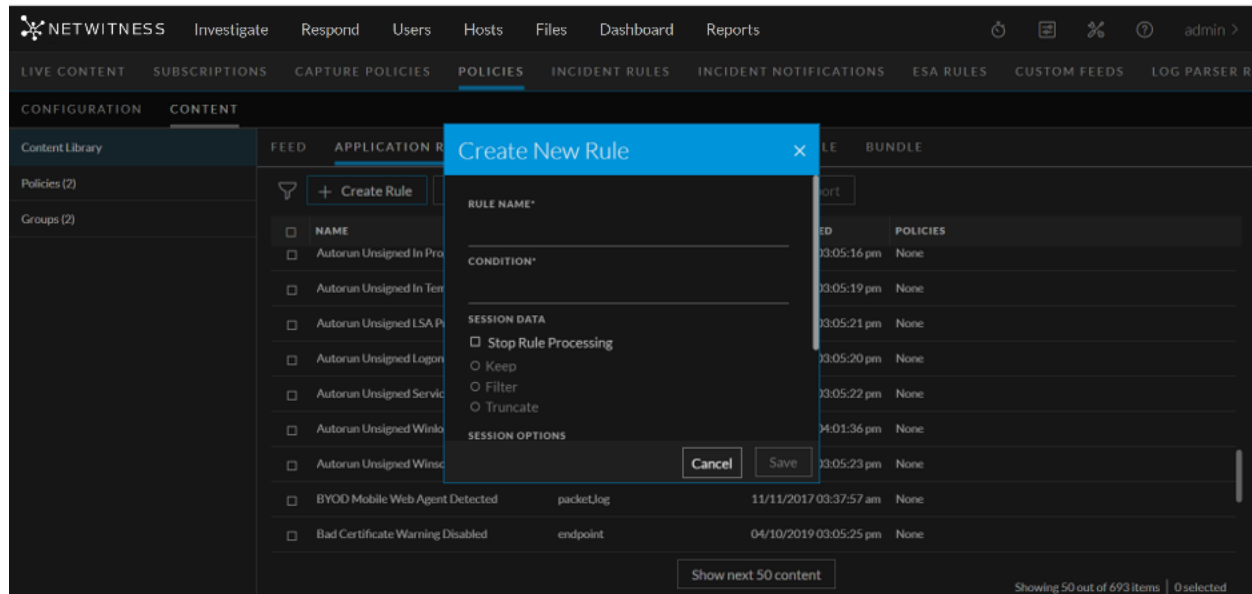
- Name - Name of the rule.
- Medium - Medium through which the rule is created.
- Last Updated - Displays the time when the rule is updated.
- Policies - Policies to which the rule is applied.

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.

### Create New Rule dialog:

Below is an example of the Create new rule dialog:

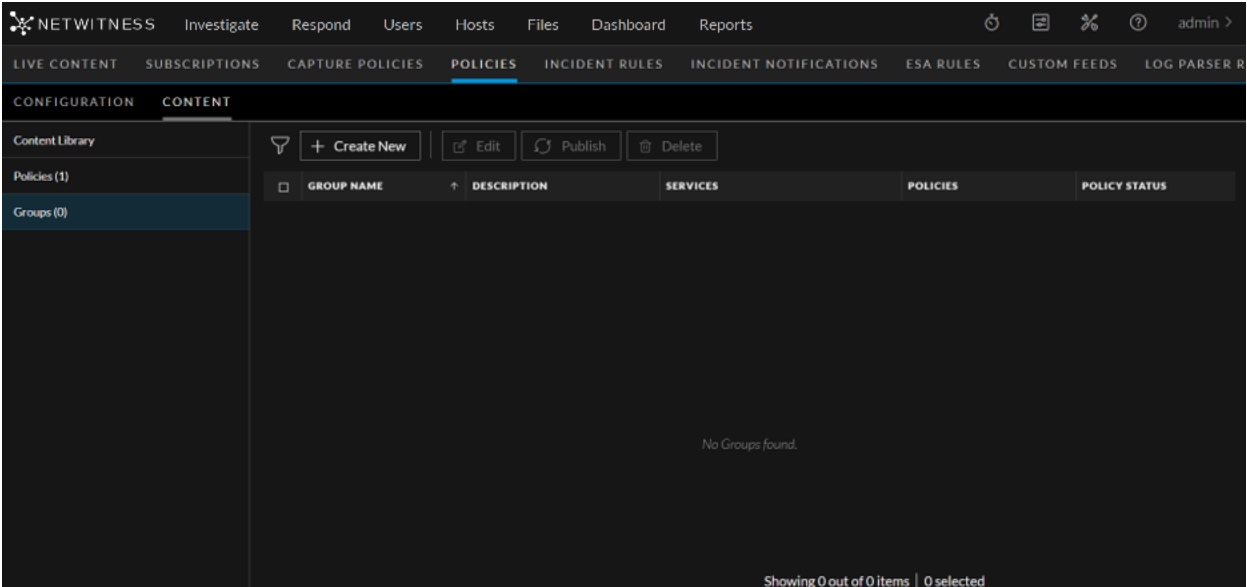


The table describes the information and options in the Create New Rule dialog:

Field	Description
Rule Name	Name of the new rule. The name should be unique.
Condition	Condition for the new rule.
Medium	Medium through which the rule is created.
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.

## 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:

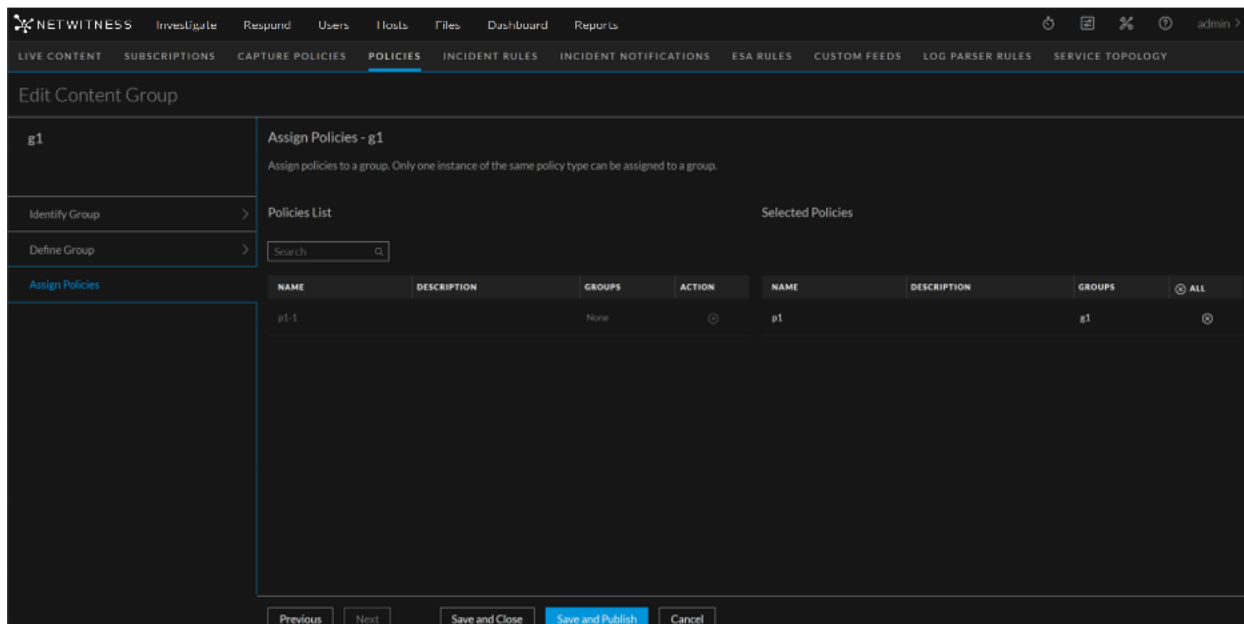
Field	Description
Group Name	Name of the group. The name should be unique.
Group Description (Optional)	Description of the group. Description should not exceed 8000 characters.
Save and Close	Saves the settings and closes the Create Group dialog.

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> <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:

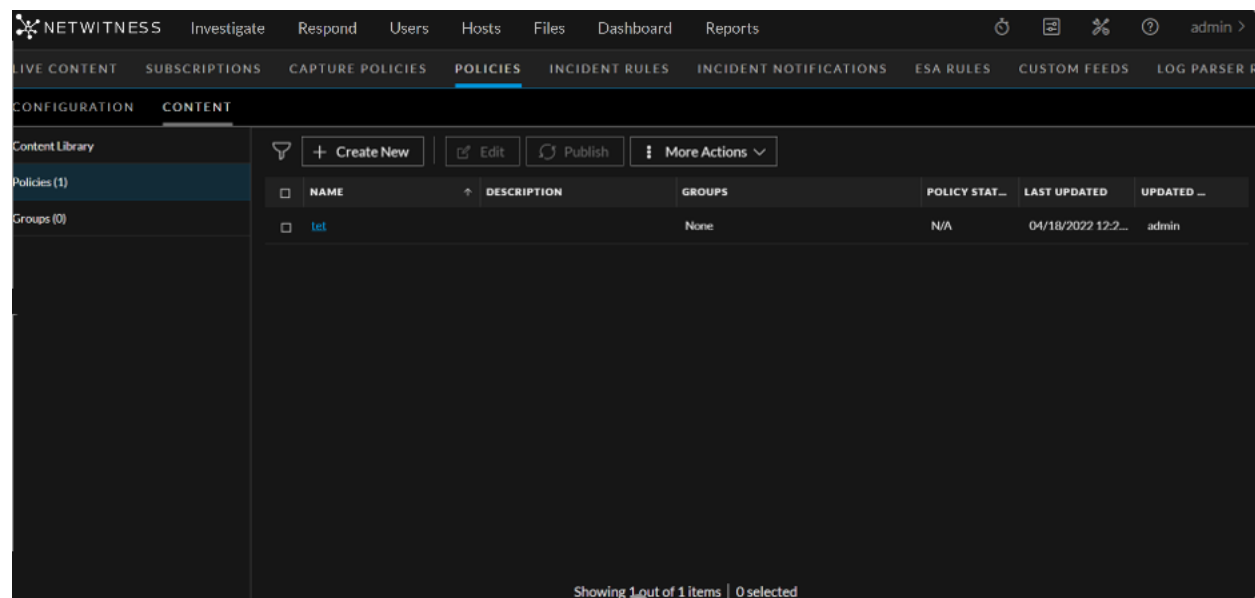
Field	Description
-------	-------------

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	<p>Saves and publishes the created group.</p> <div> <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>

## Policies Tab

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 [Managing Groups](#).
- 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.

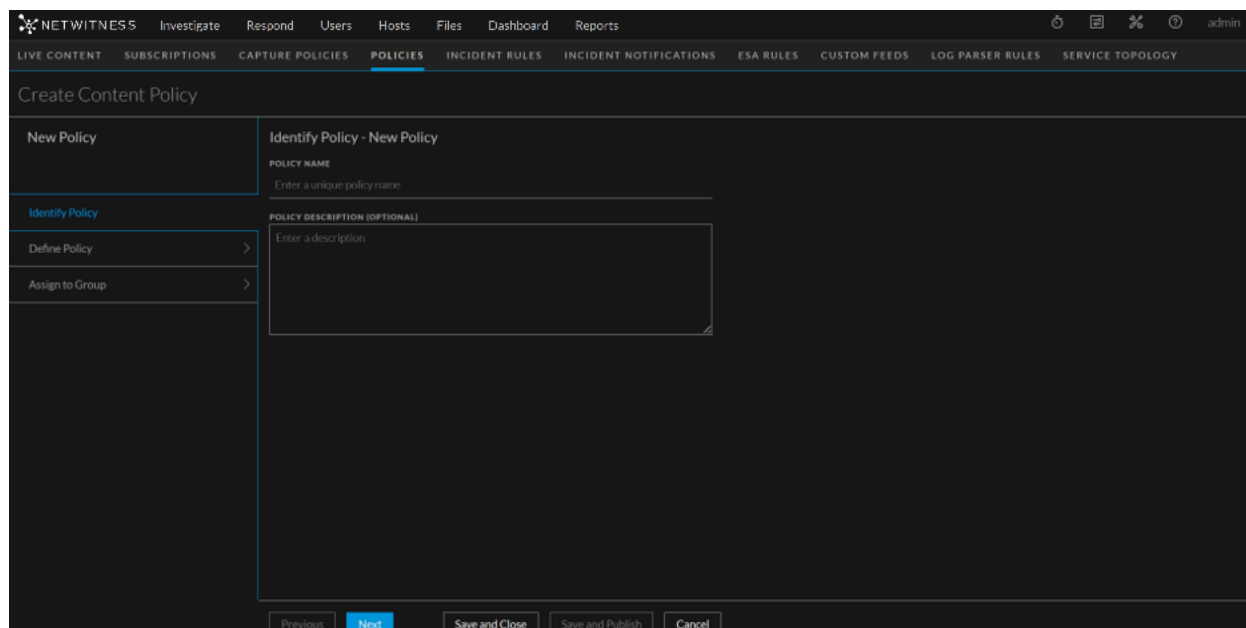
## 2 Policy List Pane:

- 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 properties of the selected policy.

Below is an example of the Create Content Policy dialog.



NETWITNESS Investigate Respond Users Hosts Files Dashboard Reports

LIVE CONTENT SUBSCRIPTIONS CAPTURE POLICIES **POLICIES** INCIDENT RULES INCIDENT NOTIFICATIONS ESA RULES CUSTOM FEEDS LOG PARSER RULES SERVICE TOPOLOGY

### Create Content Policy

New Policy

Identify Policy

Define Policy >

Assign to Group >

Identify Policy - New Policy

POLICY NAME

Enter a unique policy name

POLICY DESCRIPTION (OPTIONAL)

Enter a description

Previous Next Save and Close Save and Publish Cancel

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:

**Create Content Policy**

test

Define Policy - test

Add content along with its dependencies to the policy.

Identify Policy >

Available Content

Filters Search

Application Rule

Feed

Log Collector

Log Device

Lua Parser

Selected Content

All the dependencies are added automatically for the selected content.

Application Rule

NAME	MEDIUM	CREATED	LAST UPDATED	SUBSCRIBED	ALL
AWS-Critical charact...	log	09/14/2021 ...	09/14/2021 ...	<input type="checkbox"/>	

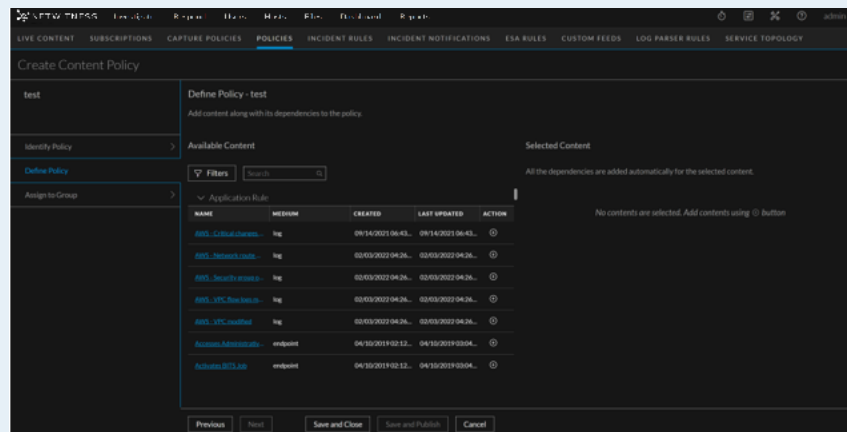
Previous Next Save and Close Save and Publish Cancel

Field	Description
-------	-------------



## Available Content

Displays the available content resources in your deployment. Click expand the resource type.



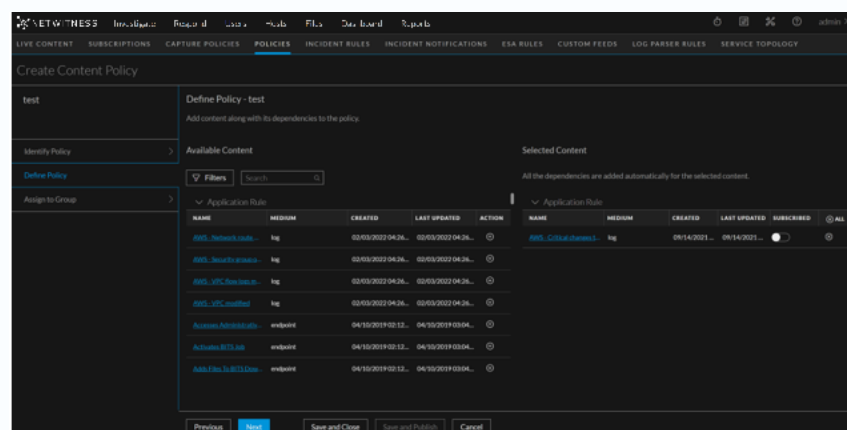
The following describes resource type:

- **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:

NETWITNESS Investigate Respond Users Hosts Files Dashboard Reports

LIVE CONTENT SUBSCRIPTIONS CAPTURE POLICIES **POLICIES** INCIDENT RULES INCIDENT NOTIFICATIONS ESA RULES CUSTOM FEEDS LOG PARSER RULES SERVICE TOPOLOGY

Create Content Policy

test

Assign to Group - test

Assign groups to the policy. A group is disabled if it is assigned to another policy.

Identify Policy >

Define Policy >

Assign to Group

GROUP NAME	POLICIES	SERVICES	ACTION
g1	p1	decoder - Decoder	⊕

No groups found. The groups are already assigned to policies.

Previous Next Save and Close Save and Publish Cancel

**Group List** Displays the list of groups associated with the policy. A group is disabled if it is already assigned to another policy.

- Group Name
- Policies
- Services
- Action

**Selected Group** Lists the selected groups. Click to add groups.

**Save and Close** Saves the settings and closes the Create Policy dialog.

**Save and Publish** Saves and publishes the created policy.

**Note:** This option is disabled if:

- Policy settings are not customized.
- Policy is not assigned to groups.

## 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 programdata directory"
- "autorun unsigned in temp directory"
- "autorun unsigned logon type registry startup method"
- "autorun unsigned lsass 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"
- "kext 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"
- "pservices runs powershell"
- "pservices runs scripting engine"
- "pservices 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"
- "tamper 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 appdatalocal directory"
- "unsigned writes executable to appdataroaming 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"