RSA NETWITNESS® SUITE

Live Services Management Guide

for Version 11.1

Contact Information

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

Trademarks

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

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, 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 Dell.

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

March 2018

Contents

Live Services Management

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

NetWitness Suite Live

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

The CMS Library

The content management system (CMS) library (known as *Live*) is a valuable source of the latest internet security resources for NetWitness Suite 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 Suite Feedback and Data Sharing

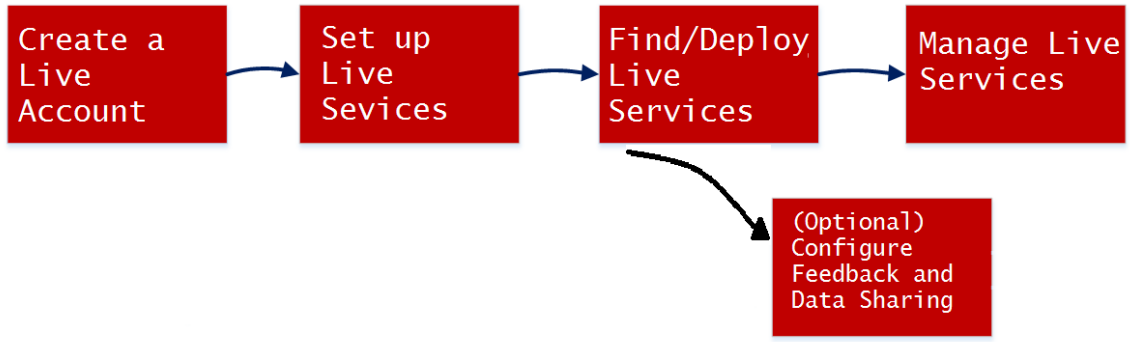
Live Feedback is intended to help improve RSA NetWitness Suite. Once you set up and configure a Live account, usage data is shared with RSA.

RSA Live Connect is a cloud based threat intelligence service. This service collects, analyzes, and assesses threat intelligence data such as IP addresses, domains, and files collected from various sources. It **Threat Insights**, which provide analysts the ability to pull threat intelligence data from the Live Connect service. It also offers **Analyst Behaviors**, an automated data collection service with the goal of sharing potential threat intelligence for analysis.

For more details, see NetWitness Suite Feedback and Data Sharing.

Live Services Required Procedures

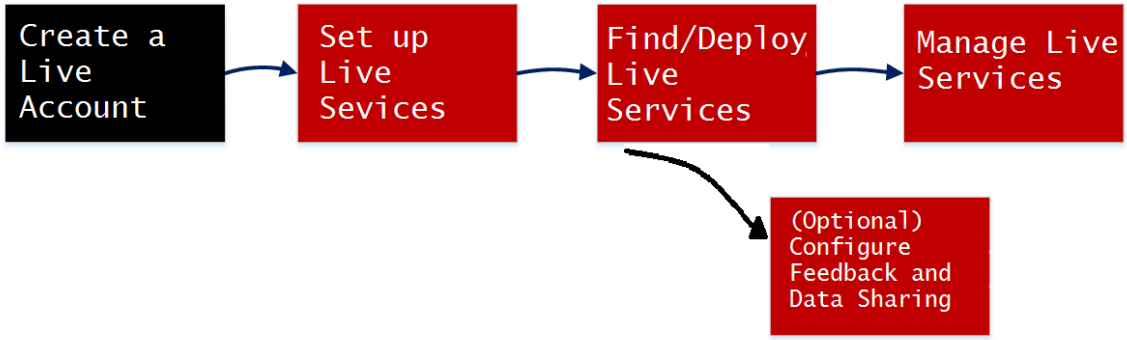
The following workflow breaks out the basic setup into four steps, which you can do individually. The easiest way to set up the Decoder is to follow the end-to-end procedure in this section, Live Services Required Procedures), which includes all of the steps.



Configuration Step	Description
Create Live Account	Create a Live Account on the RSA Live Registration portal URL: https://cms.netwitness.com/registration/. If you have an existing account, you can manage your account using this portal.
Set Up Live Services on NetWitness Suite	Set Up Live Services on NetWitness Suite by configuring a connection with the CMS server.
Find and Deploy Live Resources	Search and browse for resources in the Live Search view, an then, deploy the selected resources.
Manage Live Resources	Procedures for administrators to search for, subscribe to, and deploy resources from Live.
NetWitness Suite Feedback and Data Sharing	Describes the feedback and data sharing features provided in RSA NetWitness® Suite, from Live Services. Participation is optional, but can help to provide useful threat intelligence for the community.

Create Live Account

You must create a Live account using the RSA Live Registration Portal on the CMS server. The CMS Library provides access to all RSA content in one place where you can view, search, deploy, and subscribe to RSA content. You must register on the RSA Live Registration Portal and select a subscription level.



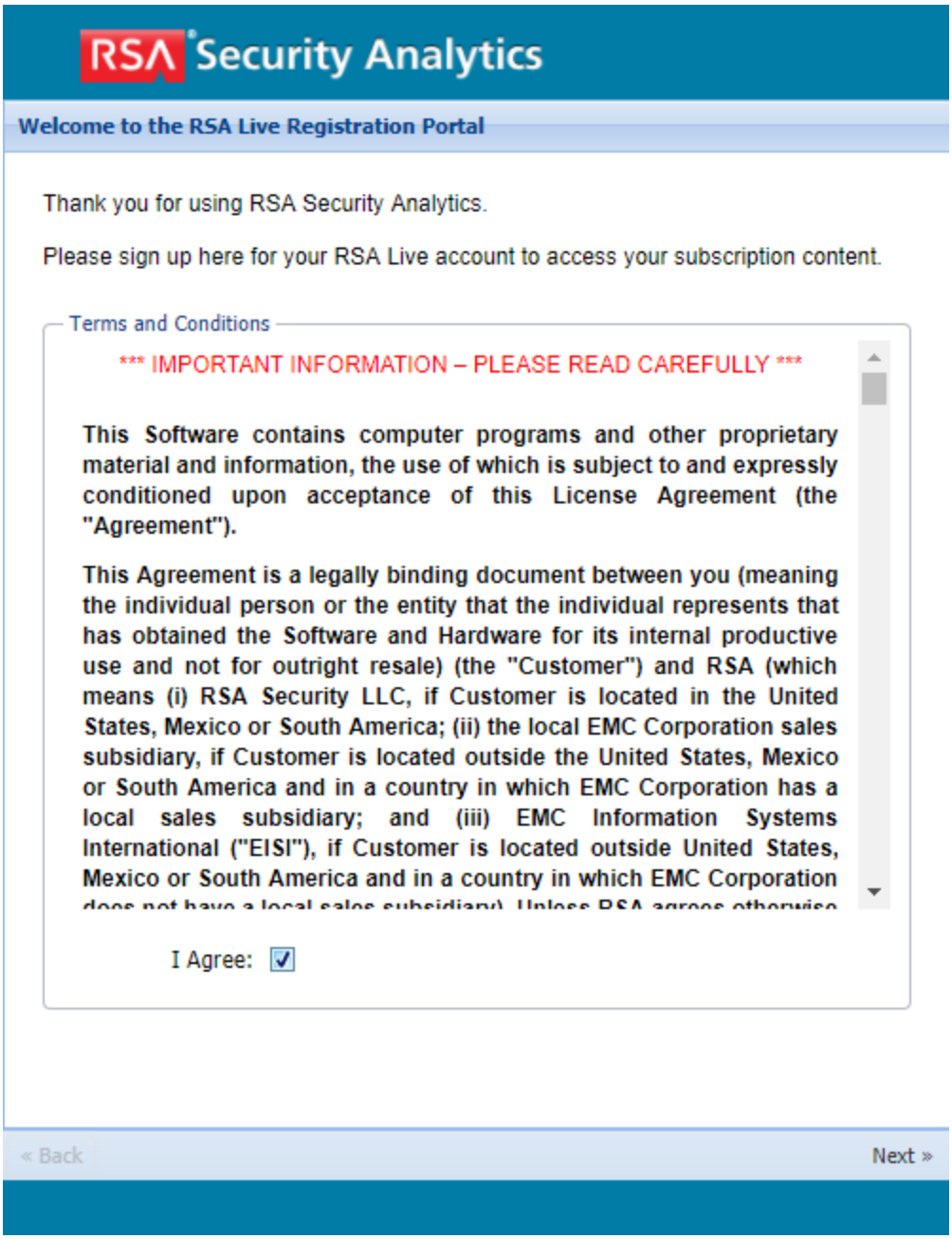
Make sure the following are available to set up a RSA Live account:

- Active internet connection to access the portal.
- A valid and registered NetWitness Suite 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 RSA customer support.

To create a Live Account:

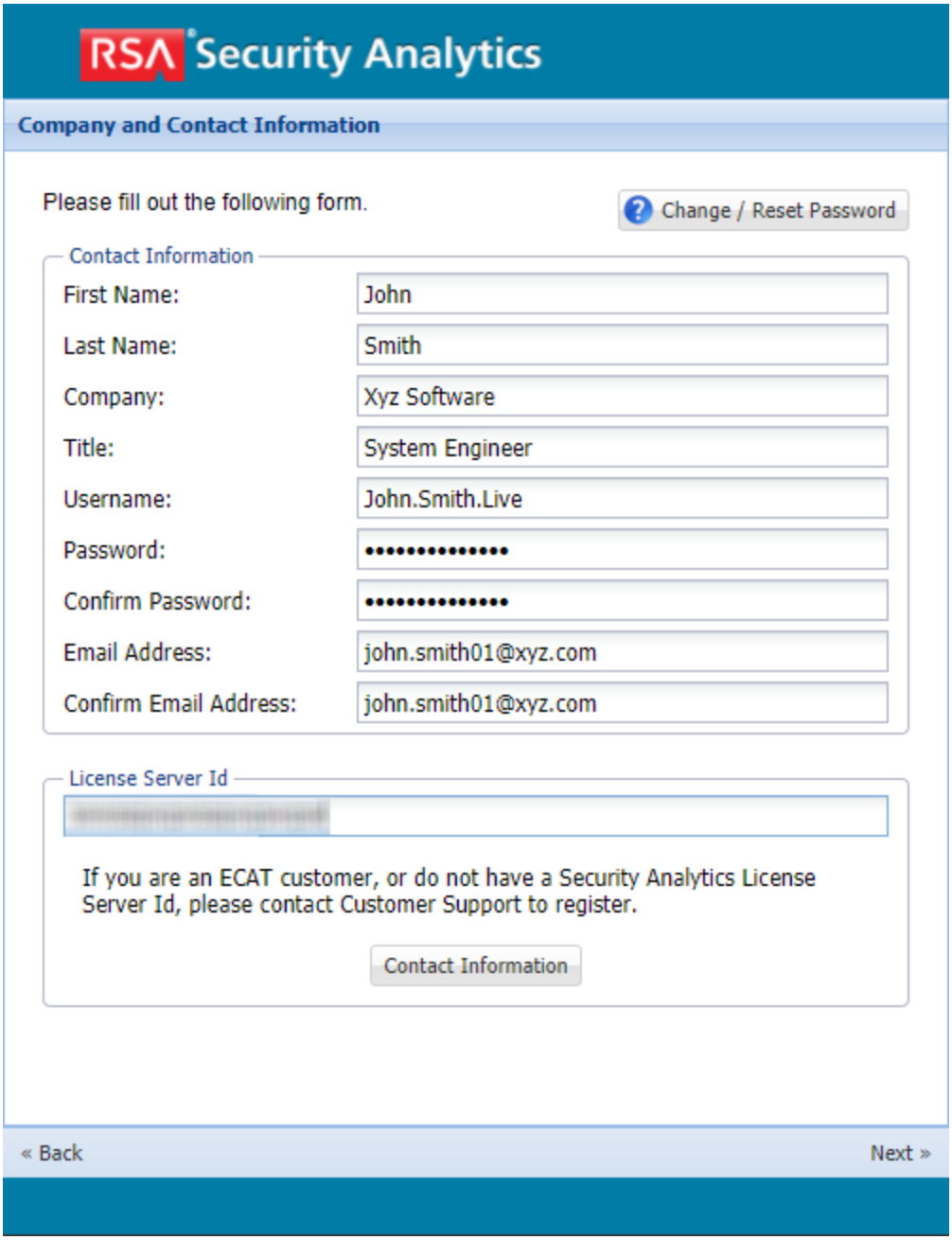
1. Access the RSA Live Registration Portal using the URL: https://cms.netwitness.com/registration/.
   The Welcome page is displayed.
2. Read the Terms and Conditions carefully and select the **I Agree** check box, as shown below:



3. Click **Next**.
4. In the **Contact Information** section, enter all the fields, as shown below:
   - The **username** must contain a minimum of nine characters and a maximum of 60 characters.
   - The **password** must contain a minimum of nine characters and a maximum of 60 characters, with at least one uppercase, one lowercase, one number, and one special

character.

- The **email address** you enter is used to send notifications related to your Live account.



5. In the **Subscription Level** section, select one of the following subscription levels:
   - **Basic** - This provides access to the Live content that is tagged for groups such as Basic, Panorama for Log Decoder, and Spectrum for Malware Analysis.
   - **Enhanced** - This provides access to the Live content that is tagged for groups such as Enhanced, Basic, Panorama for Log Decoder, and Spectrum for Malware Analysis.

- **Premium** - This provides access to the Live content that is tagged for groups such as Premium, Verisign Premium, Enhanced, Basic, Panorama for Log Decoder, and Spectrum for Malware Analysis.

6. In the **Confirm Subscription Level** section, select the subscription level once again to confirm.
7. Enter the **License Server Id**. You can view the License Id on the **ADMIN > SYSTEM > Info** page.

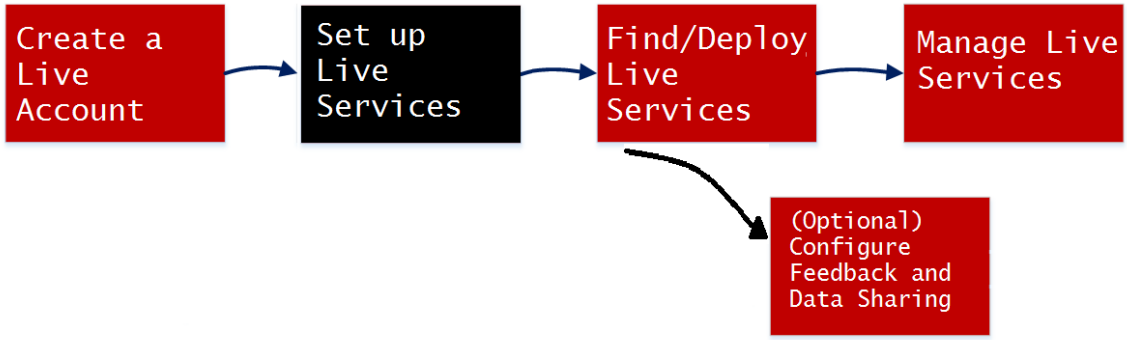
   Caution: Make sure that the license server ID on NetWitness Suite is valid and it is registered on the Flexera Server. If not, contact RSA Customer Support.

8. Click **Next**.

If the registration is successful you will receive RSA Live Account Confirmation email with your username. You now have access to the content subscribed.

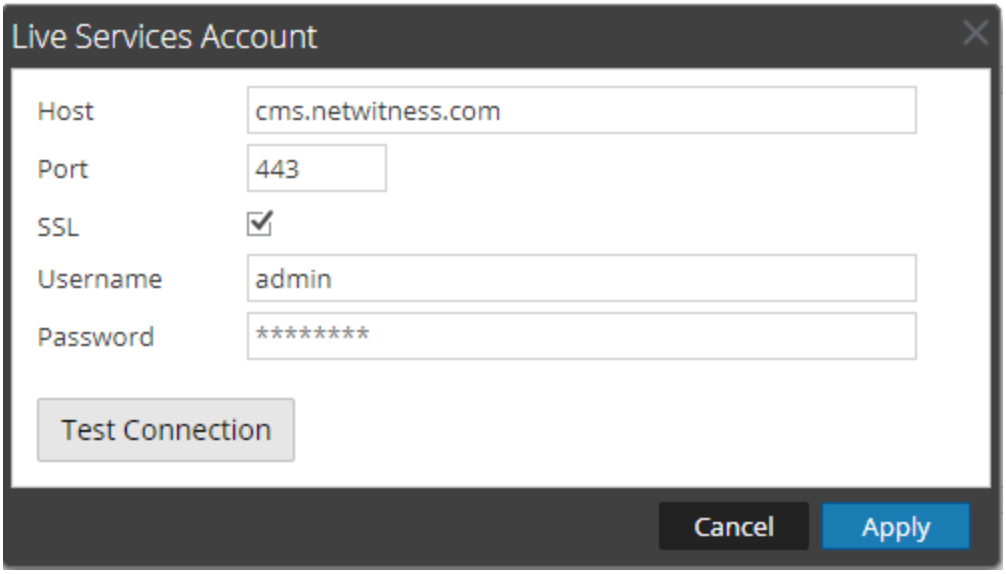
Set Up Live Services on NetWitness Suite

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



To configure the connection to the CMS Server:

1. Configure the connection to the CMS server and the Live account.

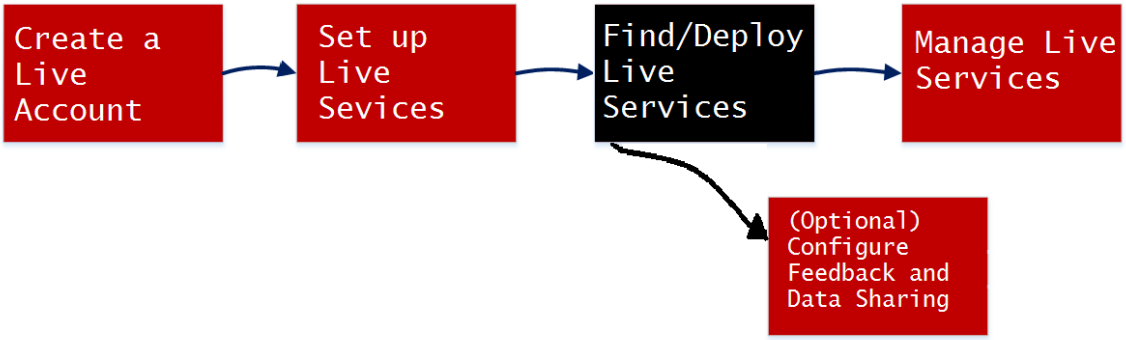


2. Configure the timing for synchronization of NetWitness Suite with updates from Live.

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

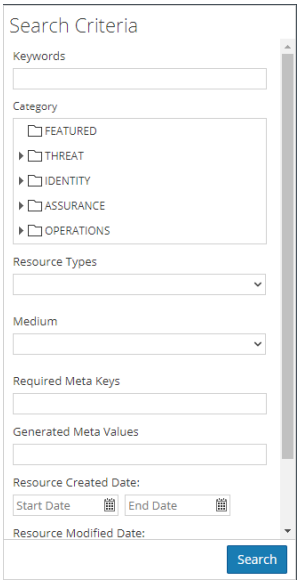
Find and Deploy Live Resources

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.



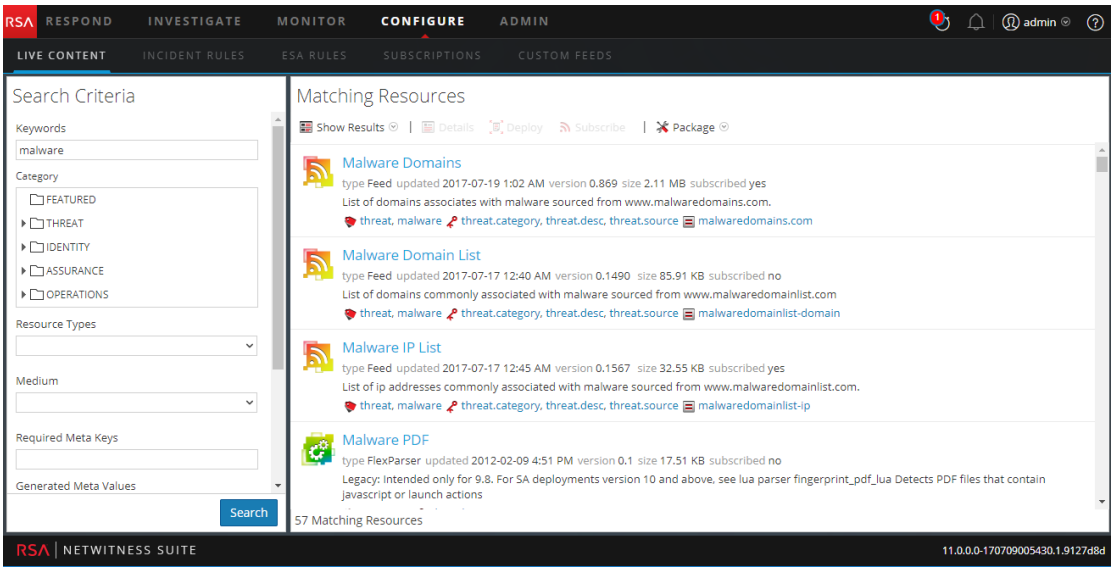
Find Resources

1. 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.



2. Click **Search**.

   Detailed results are shown in the Matching Resources panel.



3. (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 RSA NetWitness Suite, 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 Suite Live, you can deploy resources manually to a service or a service group without subscribing to the resources.
- Deploying resources manually deploys to services without taking advantage of the powerful resource management capabilities of NetWitness Suite. 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.

For manual deployment, this is the basic procedure:

1. Select a resource or group of resources, or select a previously-created package of resources.
2. Click Deploy, which starts the Deployment Wizard.
3. Review the list of selected resources.
4. Select the Services or Service Groups on which to deploy the selected resources
5. Review your previous selections
6. Deploy

The following procedure describes how to deploy a group of resources or a resource package:

- You can select one or more resources in the Live Resource View , then deploy them to services.
- Or, 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.

To deploy resources manually:

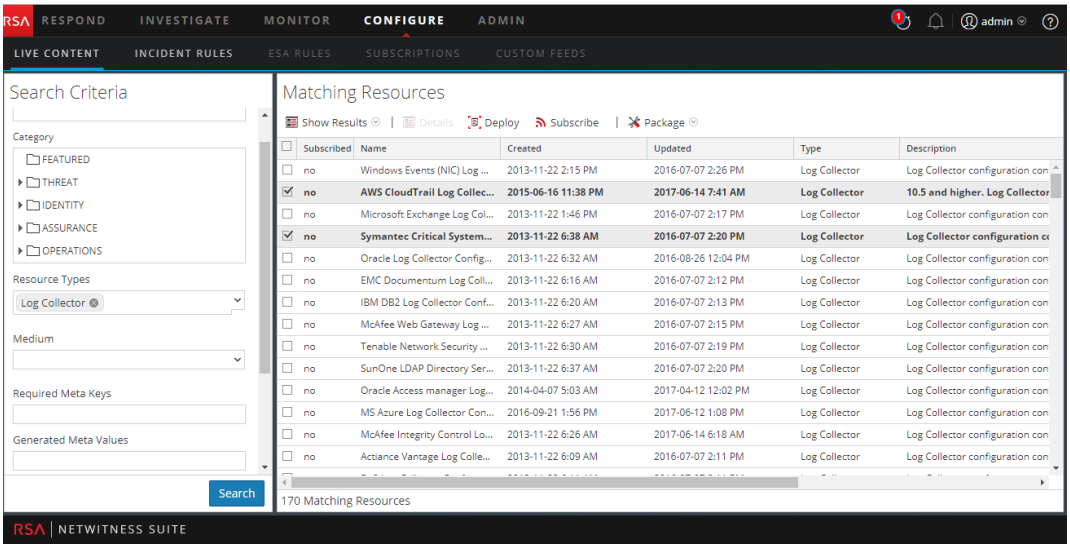
1. Go to **CONFIGURE > Live Content**.
2. Select a group of resources, or a previously created resource package.

   To select a resource or group of resources:

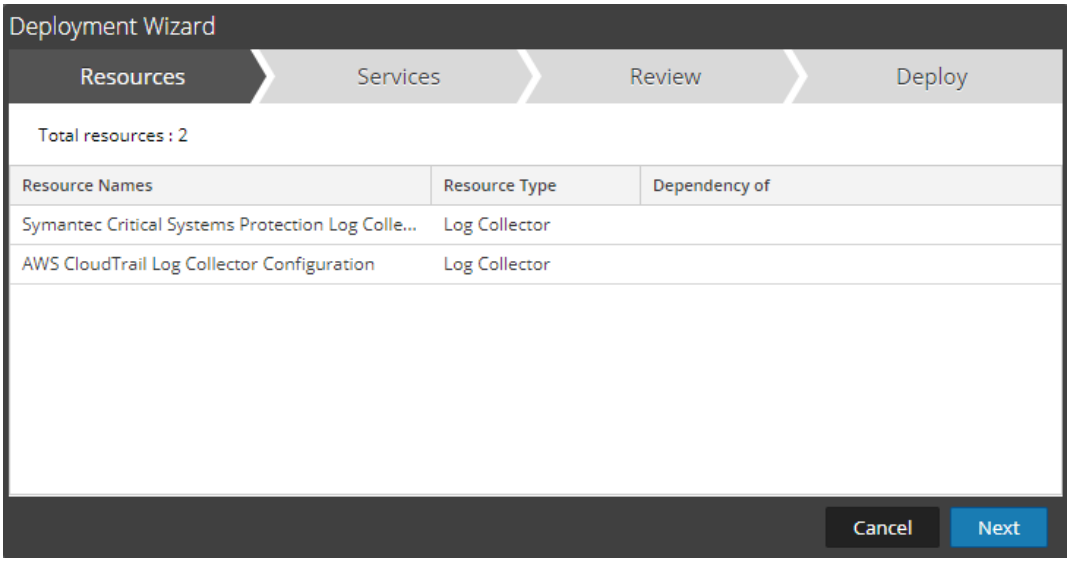
   a. In the **Live Search View,** browse Live resources (for example, search for the **Log Collector** resource Type).

   b. In the **Matching Resources** panel, select **Show Results > Grid**.

   c. Select the checkbox to the left of the resources that you want to deploy.



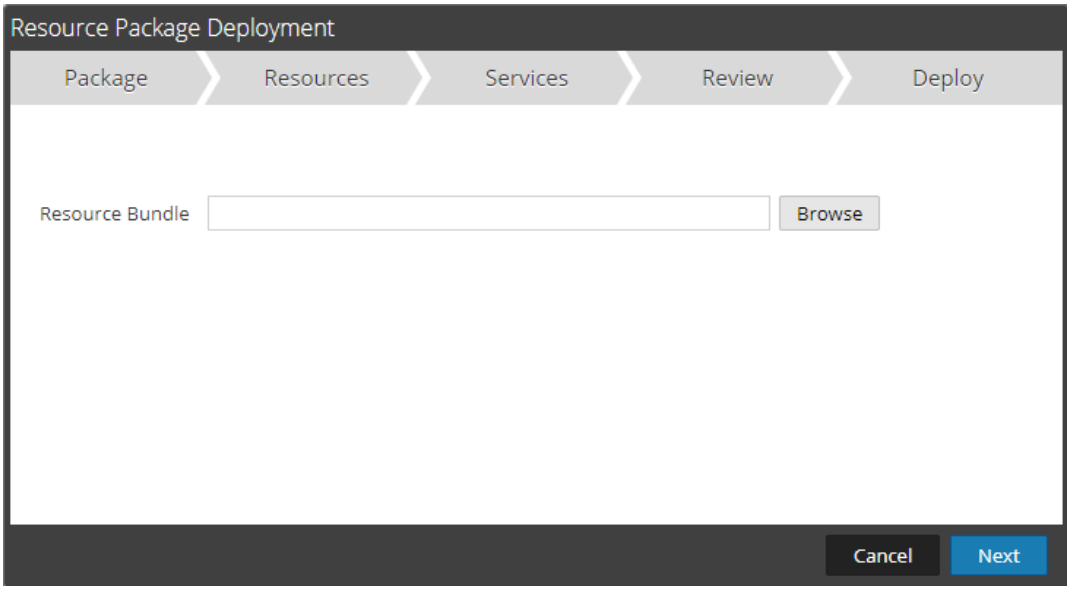
d. In the Matching Resources toolbar, click Deploy.



3. To select a resource package to deploy:

a. In the **Live Search** view **- Matching Resources** toolbar, select **Package** > **Deploy** :

The Package page of the Resource Package Deployment wizard is displayed.



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

c. Click **Open**.

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

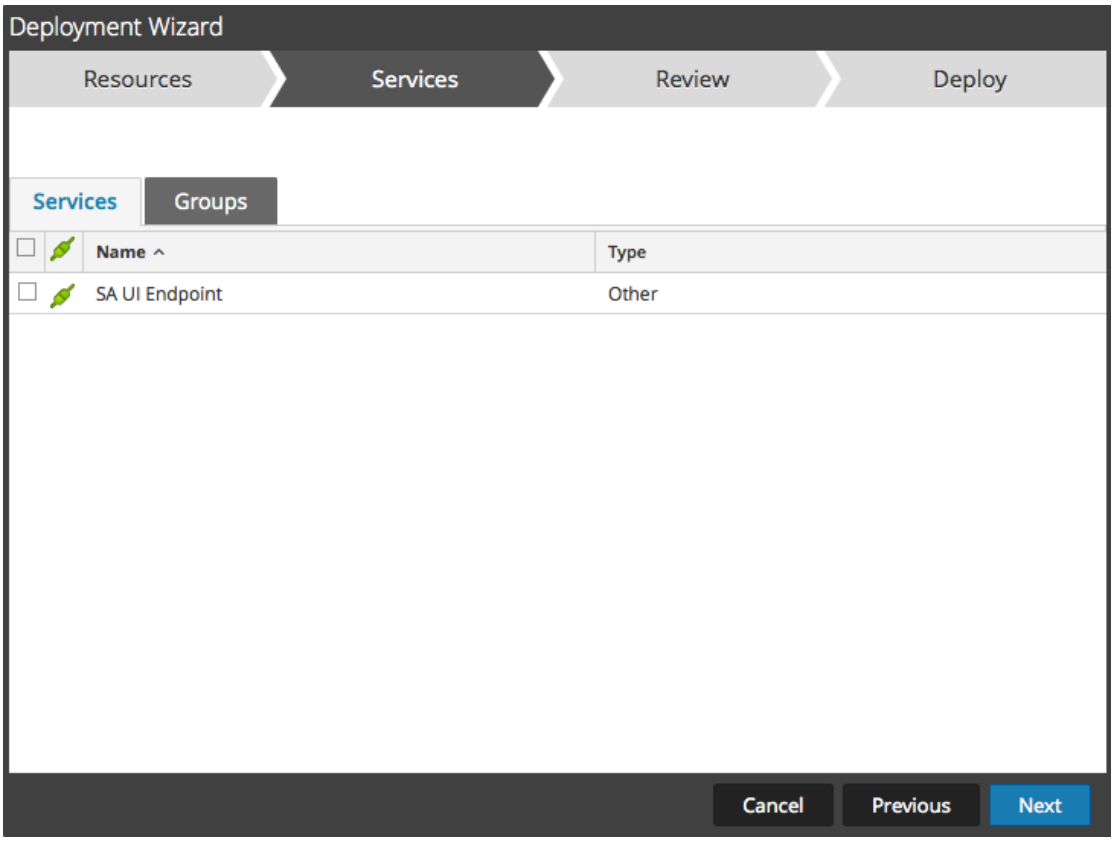
4. Click **Next**.

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

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

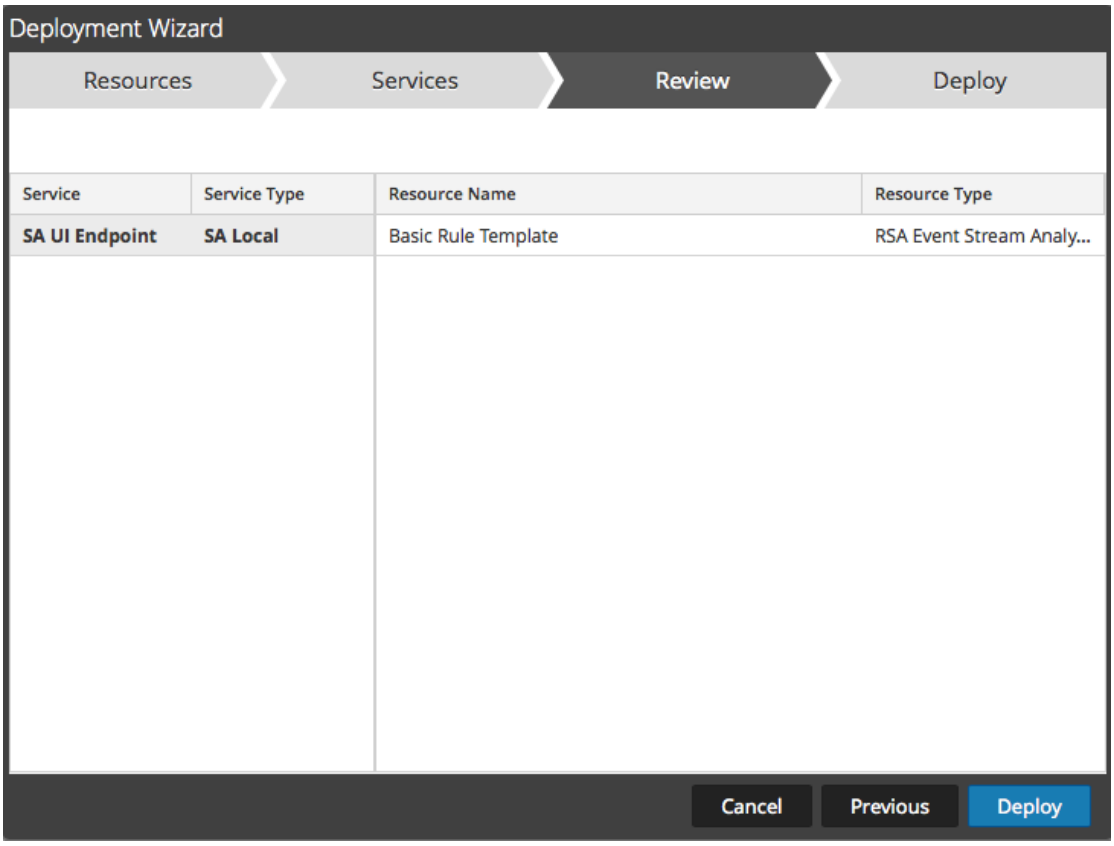
5. Select the services to which you want to deploy the content. You can select any combination of services and service groups.

   - Use the **Services** tab to select individual services, list of services and service groups that are configured in the ADMIN Services view.
   - Use the **Groups** tab to select groups of services



6. Click **Next**.

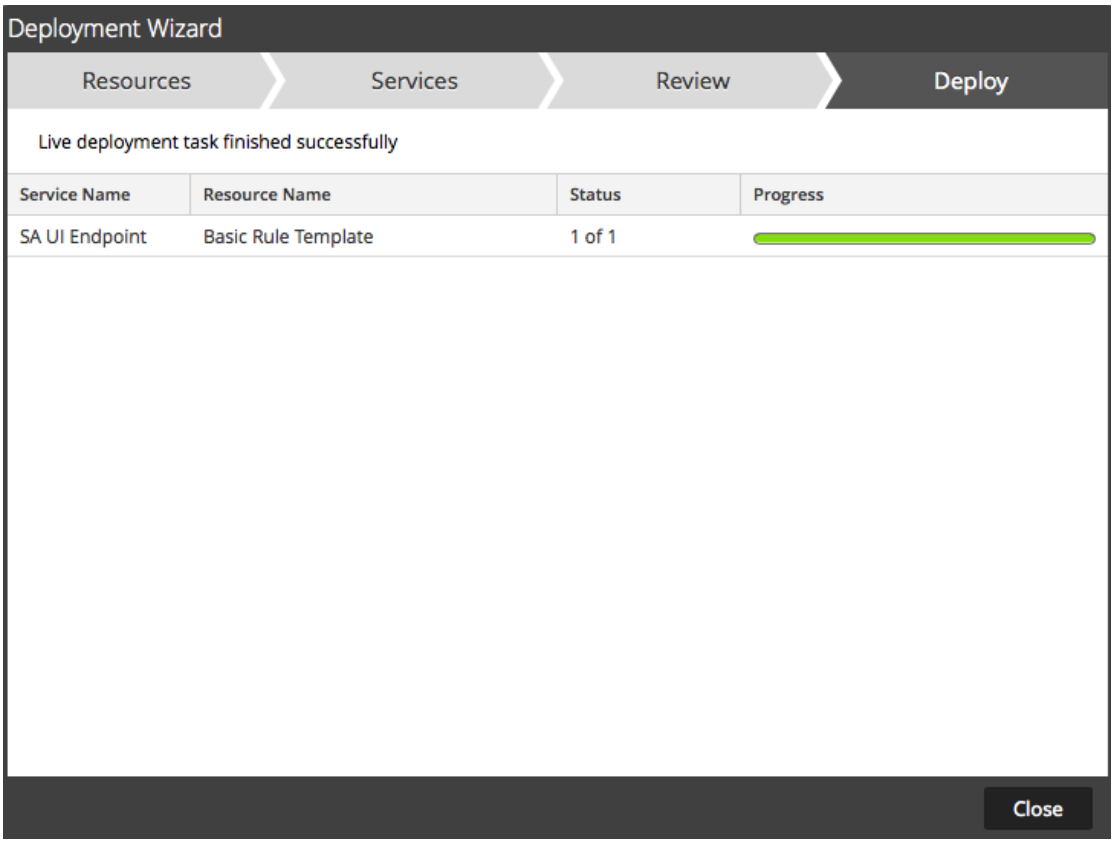
   The **Review** page is displayed.



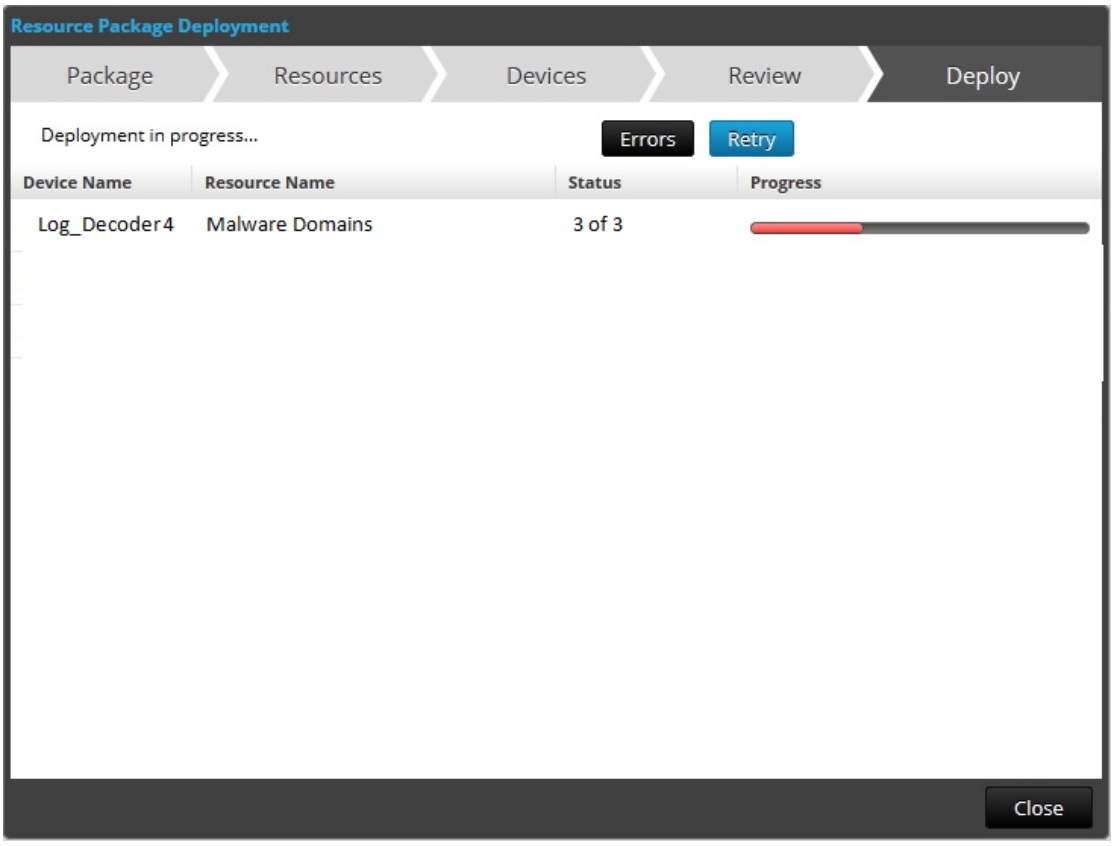
Make sure that you have selected correct resources and the services to which you want to deploy them.

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 Suite displays the Errors and Retry buttons, which you click to review the errors and re-attempt the deployment.



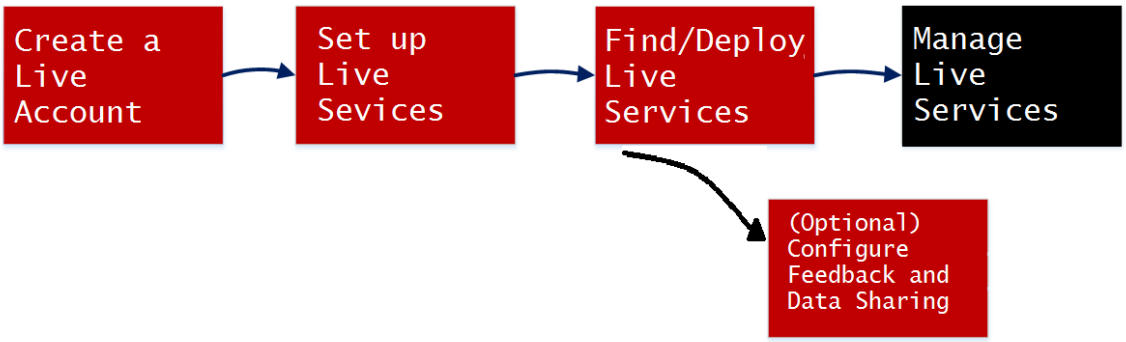
8. Click **Close**.

Next steps

After deploying parsers to Decoders and Log Decoders, you must enable parsers on the individual services as described in the *Decoder and Log Decoder Configuration Guide*.

Manage Live Resources

These procedures are required when administrators want to search for, subscribe to, and/or deploy resources from Live. 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 Admin Services view.



Procedures

There are several possible 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.

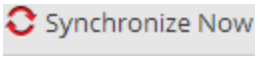
Manage Subscription and Deployment

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 > Live Configuration** panel.

By adding subscribed resources to the deployments list, you configure NetWitness Suite 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** panel, specify an interval at which NetWitness Suite 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 **Live** > **Search** view, search for and subscribe to Live resources.
3. In the **Live** > **Configure** view > **Deployments** tab, select subscribed resources and add them to the deployment list for services groups.
4. (Optional) In the **ADMIN**> **SYSTEM**> **Live** panel, click 

to deploy the resources listed in the Deployments tab immediately.
5. In the **Live** > **Configure** view > **Deployments** tab, select deployed resources and remove them from services groups.
6. In the **Live** > **Configure** view > **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 resources, go to the Live Resource View, unsubscribe from a resource, and remove the resource from services where it is deployed.

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 Suite 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.

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
  - Create a Custom Feed
  - Create a STIX Custom Feed
  - Create and Manage an Identity Feed
  - Edit a Feed
  - Remove a Feed
- Miscellaneous Live Services Procedures

Export Data to RSA

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

About Live Feedback

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*.

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.

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

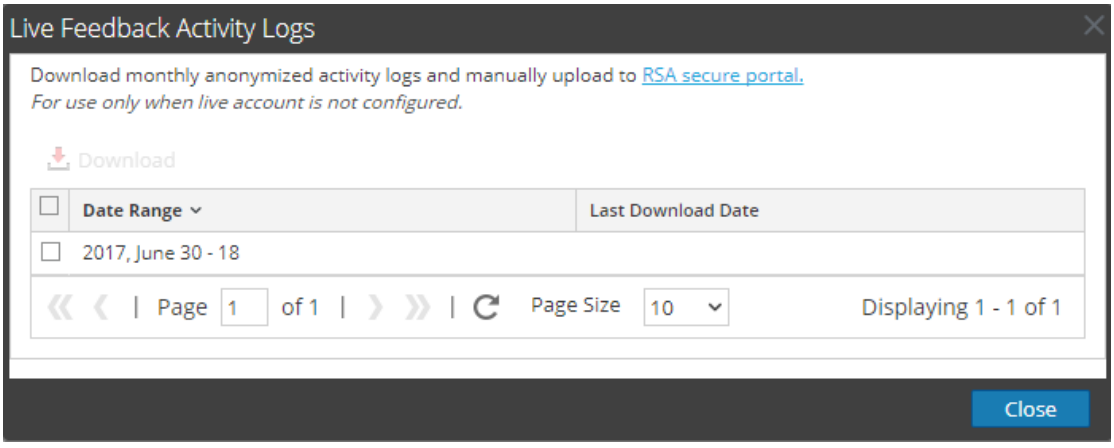
Download Live Feedback Historical Data

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 **Download Live Feedback Activity Log**.

   The **Download 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 downloaded zip file consists of an individual JSON file for each month.

The downloaded Live Feedback data is in JSON format, and is bundled as a .zip file. For more information, see "Live Feedback Overview" in the *System Configuration Guide*.

Share Data to RSA

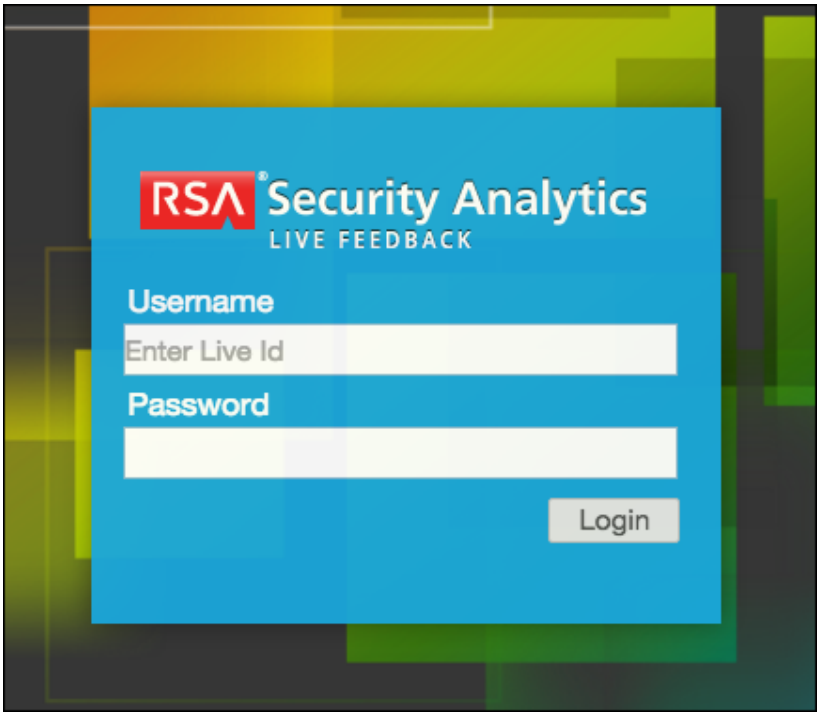
After you download the Live Feedback data, you can then upload it using the following procedure.

To share the data to RSA:

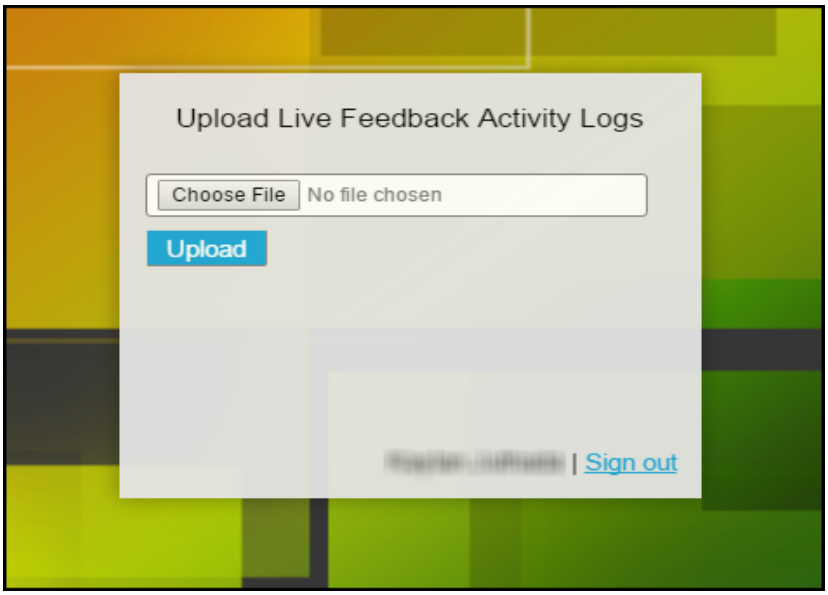
1. Click on the **RSA Secure Portal** available on the **Live Feedback Activity Logs** window.

   The RSA NetWitness Suite Live Feedback log on screen is displayed.

2. Log on to the Upload Live Feedback Activity Logs portal using your Live ID credentials.



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



4. Click **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 the more secure network.

Create and Deploy Resource Package Use Case

The basic steps are as follows:

1. Access NetWitness Suite 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 Suite instance, by using a thumb drive or other manual copying process.
4. On the secure NetWitness Suite instance, deploy the resource package. Details for this procedure are in Resource Package Deployment Wizard.

Prerequisites to Create a Resource Package

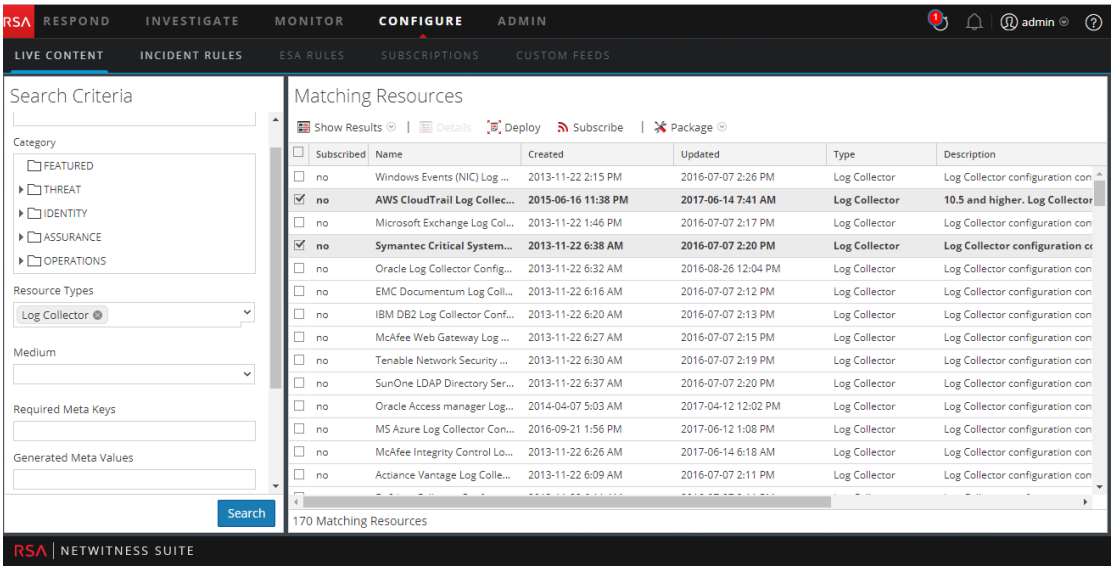
A prerequisite for creating resource packages is configuration of the connection and synchronization between the CMS server and NetWitness Suite and the ability to search for resources in the User Interface.

Procedure to Create a Resource Package

The following procedure creates a resource package, as a ZIP archive, which is saved to your local file system.

To create a resource package:

1. Navigate to CONFIGURE > Live Content from the RSA NetWitness UI.
2. Select the resources that you want to package in the Matching Resources grid.



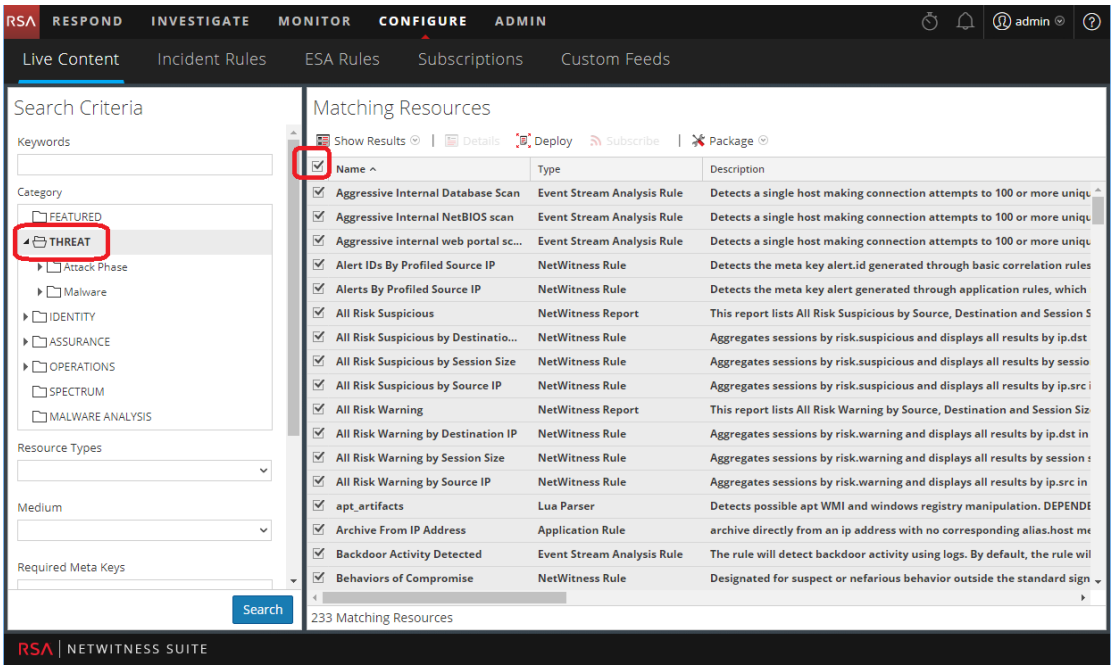
3. Select some or all of the resources that are listed in the Matches Resources pane.
4. Select Package > **Create**.

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

Example: Create Threat Package

In this example, we 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. Navigate to CONFIGURE > Live Content from the RSA NetWitness UI.
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.



4. Select Package > **Create**.

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

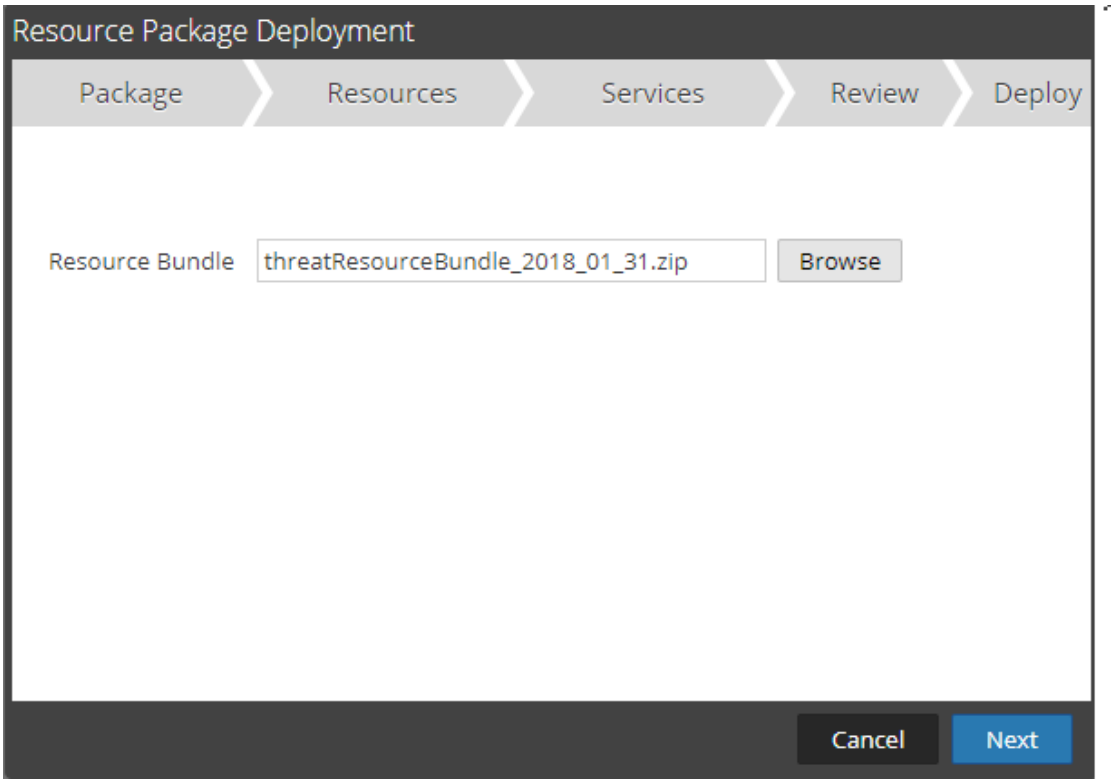
5. Rename the package to something meaningful. For example, in this case, you cold change the package name to **threatResourceBundle_2018_01_31.zip** (assuming today's date is January 31, 2018).

The resource package is now available for later deployment.

Example: Deploy Threat Package

Continuing the previous example, we deploy the resource package that we created.

1. Navigate to CONFIGURE > Live Content from the RSA NetWitness UI.
2. In the **Matching Resources** pane, select Package > **Deploy**.
3. Click Browse and navigate to the **threatResourceBundle_2018_01_31.zip** file that we created earlier.



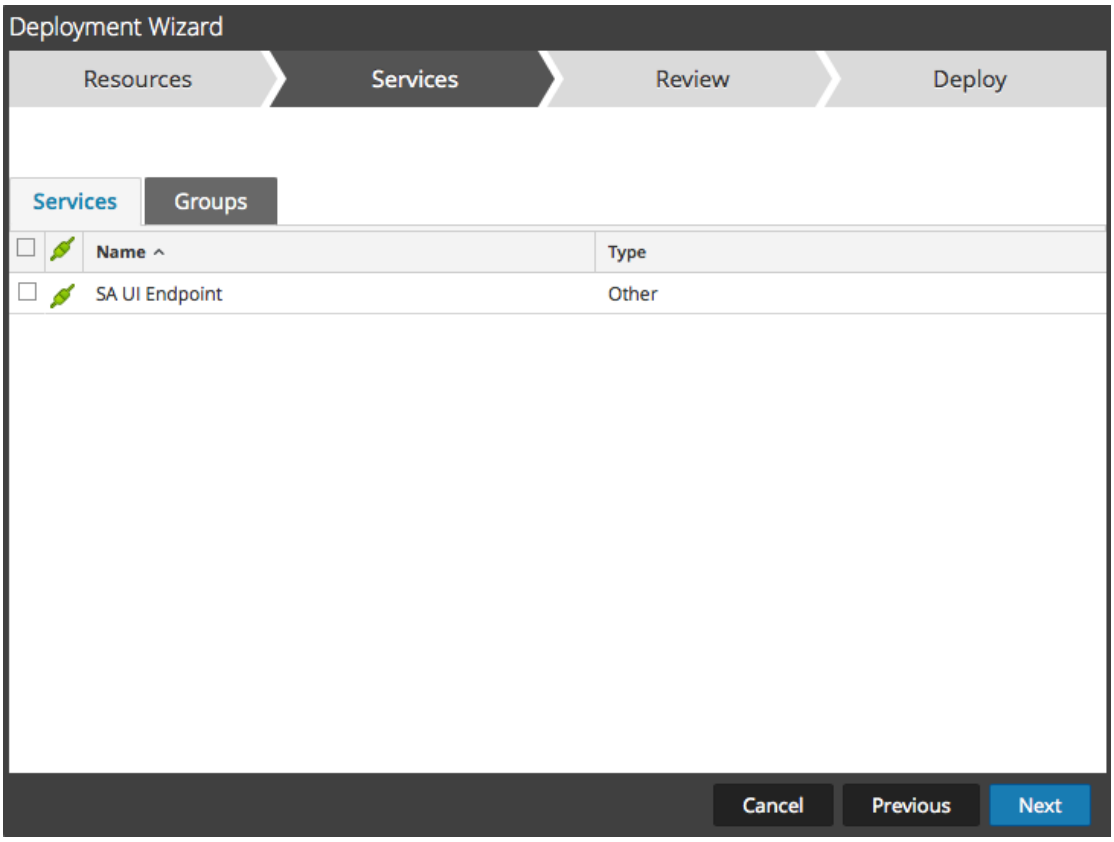
4. Click **Next**.

   The **Resources** page is displayed, showing details for the resources in the package.

5. 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.

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



Click **Next**.

The **Review** page is displayed.

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

7. 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

This topic introduces the custom feed capability, which is implemented using the Custom Feed Wizard in RSA NetWitness Suite, to quickly populate Decoders with custom and identity feeds.

Custom Feed Creation

You use the **Live** > **Feeds** > **Setup Feed** > **Configure a Custom Feed** wizard to quickly 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 RSA NetWitness Suite are in the form `<filename>.feed`. To create a feed, NetWitness Suite 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 Suite can fetch the most current version of the file for each recurrence. After a NetWitness Suite feed is created, you can download the feed to your local file system, edit the feed files, and then edit the NetWitness Suite 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 Suite 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).

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

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

</FDF>
```

Feed Definition Equivalents for Custom Feed Wizard Parameters

The NetWitness Suite 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 Suite Parameter	Feed Definition File Equivalent
Define Feed tab	
Feed Type	Select: **Default** - to define a feed based on a `.csv` formatted feed data file. **STIX** - to define a feed based on STIX formatted `.xml` file.
Feed Task Type	Select: **Adhoc** - to create an on-demand feed. **Recurring** - to create a feed that recurs automatically.
Name	The custom feed name in the feed data file. It corresponds to the **`flatfeedfile name`** attribute in the feed definition file; for example, Dynamic DNS Test Feed.
File/ Browse	This is the name of the feed data file. It corresponds to the **`flatfeedfile path`** attribute in the feed definition file; for example, dynamic_dns.csv.

NetWitness Suite Parameter	Feed Definition File Equivalent
(STIX, Recurring) **Trust All Certificate**	Select **Trust All Certificate**, if you do not want to validate the REST server certificate. This option is enabled by default (checked).
(STIX, Recurring) **Certificate/Browse**	For client authentication with the REST URL, in the **Certificate** field, click **Browse** and select the self signed certificate. The supported certificate formats are .cer, .crt with Base64 & DER encoded files.
	Define Feed tab - Advanced Options
XML Feed File	The name of the feed definition file, for example, `dynamic_dns.xml`.
Separator	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.
Comment	The character used to identify a comment in the feed data file. It corresponds to the **`flatfeedfile comment`** attribute in the feed definition file; for example, #.
Remove STIX data older than	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.
Select Services tab	Select the services to which you want to send the data feed.
(Define Columns tab, Define Index) **Type**	The type of lookup value in the index position of the feed data file. **IP** 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). **IP Range** 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). **Non IP** 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.

NetWitness Suite Parameter	Feed Definition File Equivalent
(Define Columns tab, Define Index) **CIDR**	Specifies that the IP value in the lookup position is in CIDR format. The **CIDR** attribute sets the IP address format in the field to Classless Inter-Domain Routing (CIDR) notation.
(Define Columns tab, Define Index) **Service Type**	For a Non IP index, the integer service type to filter meta lookups. It corresponds to **MetaCallback apptype** attribute in the feed definition file. A value of **0** indicates no filtering by service type.
(Define Columns tab, Define Index) **Truncate Domain**	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 **MetaCallback truncdomain** attribute. If the value is www.example.com, it is truncated to example.com. A value of **False** selects no truncation, and **True** selects truncation.
(Define Columns tab, Define Index) **Callback Keys**	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 **MetaCallback name** 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.
(Define Columns tab, Define Index) **Index Column**	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 **Field index** attribute in the feed definition file. A field with an index of **1** is the first entry in a row, the second field has an index of **2**, the third field has an index of **3**, and so on. You can select multiple index columns, if the **Feed Type** is **STIX** and **Index Type** is **Non IP**. When you select multiple index columns the values from all the selected columns are merged in the first index column that you selected.

NetWitness Suite Parameter	Feed Definition File Equivalent
(DEFINE VALUES) **Key**	The name of the **LanguageKey**, as defined in the feed definition file, for which meta is created from this row of the feed data file. It corresponds to the **Field key** attribute in the feed definition file. A key applies only to a field whose type is set to **value**. In the feed definition file, there is a list of LanguageKeys from **index.xml**, or a summary name if Source Name and Destination Name are used. For example, **reputation** is a summary name for **reputation.src** and **reputation.dst**). This value is referenced by the Field key attribute.

Next steps

- Create a Custom Feed
- Create and Manage an Identity Feed
- Edit a Feed
- Remove a Feed

Create a Custom Feed

This topic provides instructions for creating a custom feed using a .csv or STIX formatted feed data file in RSA NetWitness Suite.

Note: From 10.6.1 or later, NetWitness Suite supports Structured Threat Information Expression (STIX). 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.

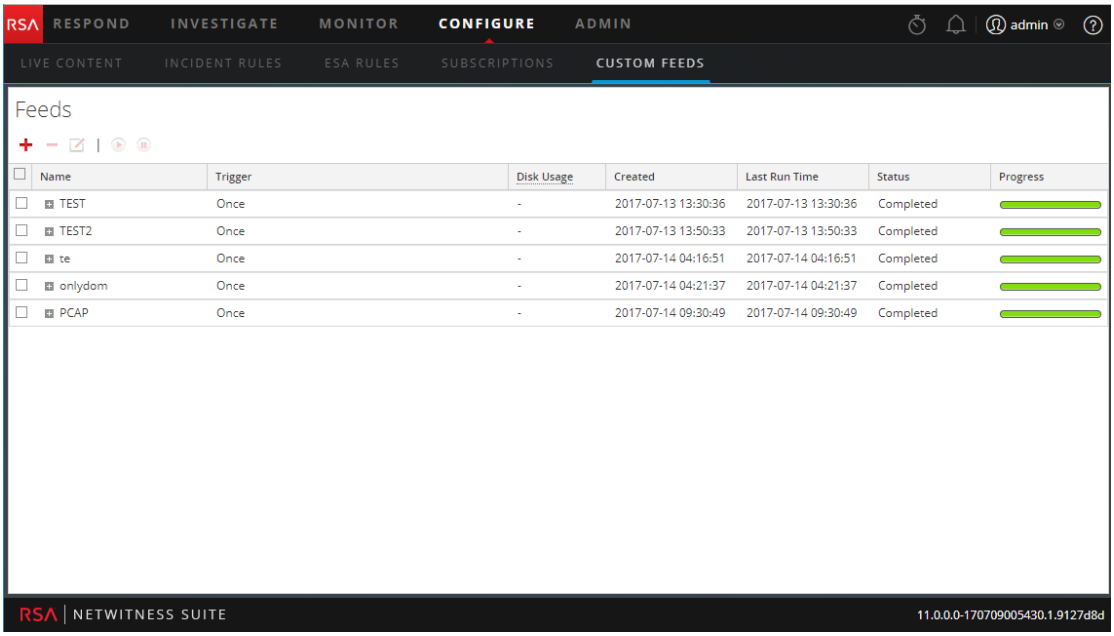
After completing this procedure, you will have created a custom feed.

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 Suite server.

To create a custom feed:

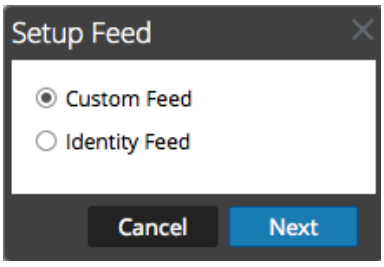
1. Go to t **CONFIGURE > CUSTOM FEEDS**.

   The Custom Feeds view is displayed.



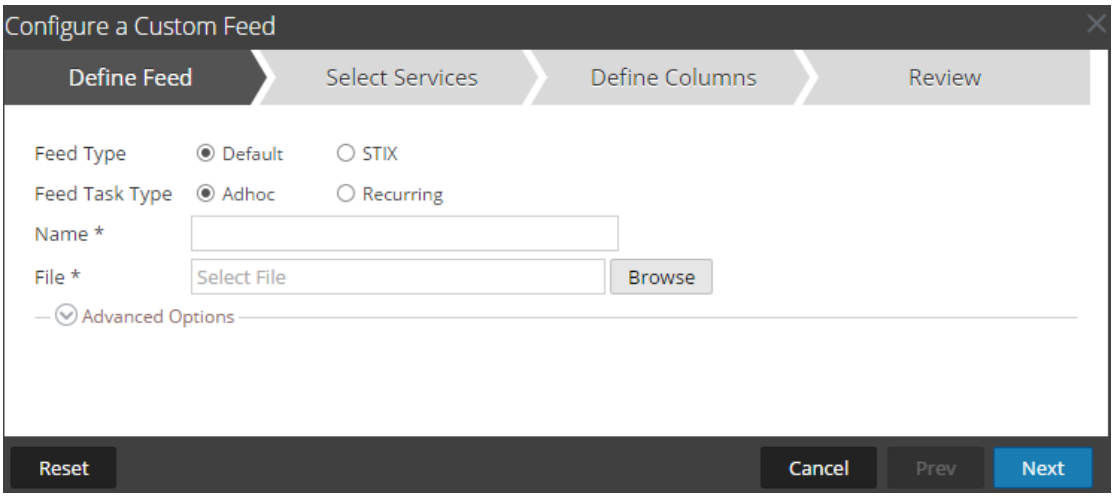
2. In the toolbar, click +.

   The Setup Feed dialog is displayed.



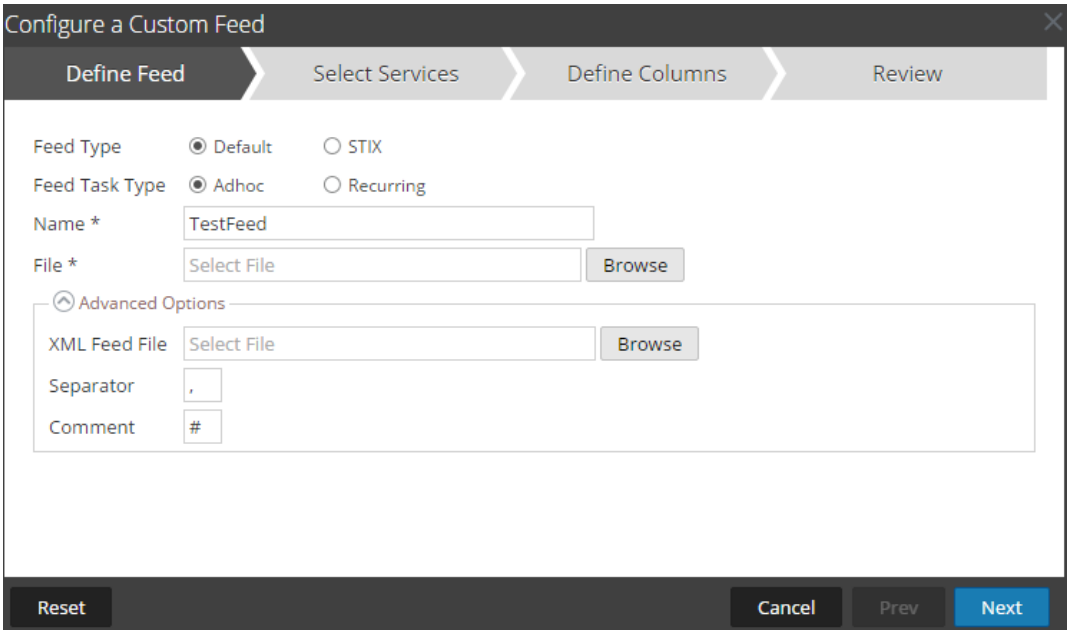
3. To select the feed type, click **Custom Feed** and **Next**.

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



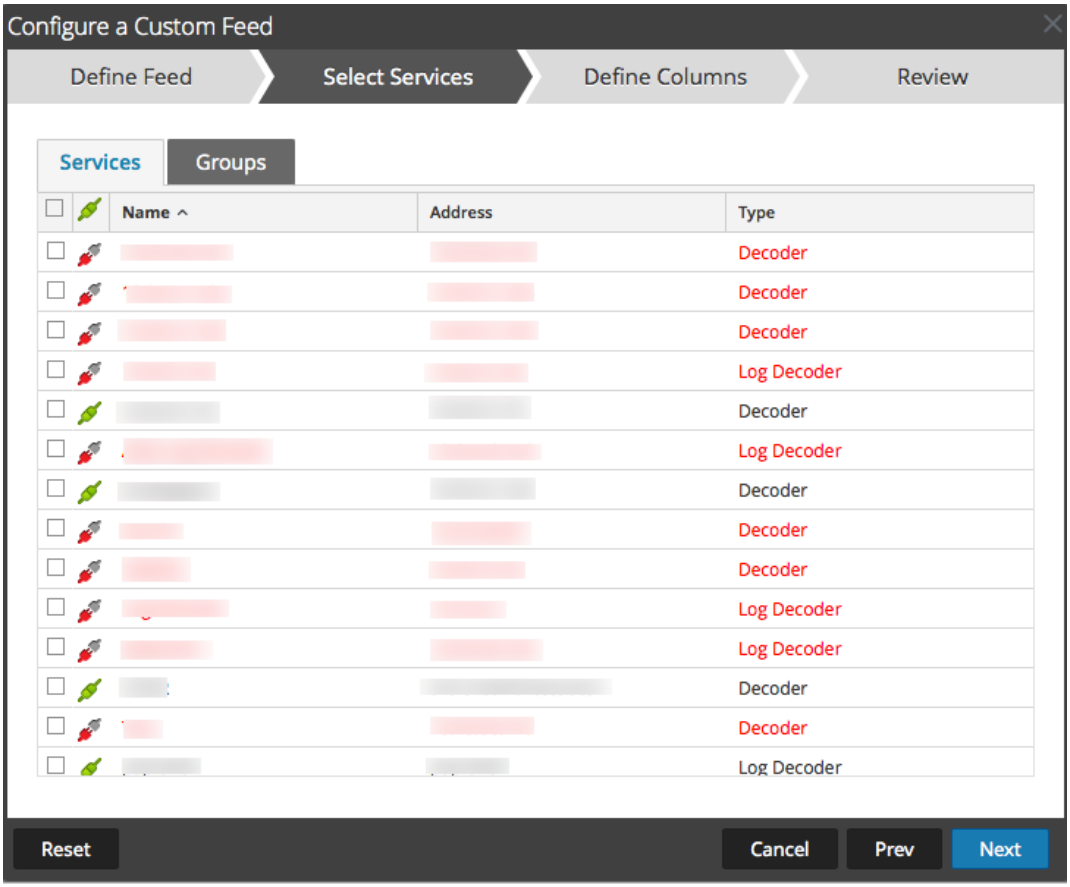
4. To define a feed based on a `.csv` formatted feed data file, select **Default** in the **Feed Type** field.
5. To define an on-demand feed task that executes once, select **Adhoc** in the **Feed Task Type** field and do one of the following:
   a. (Conditional) To define a feed based on a .csv formatted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

      The Advanced Options are displayed:



c. 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**.

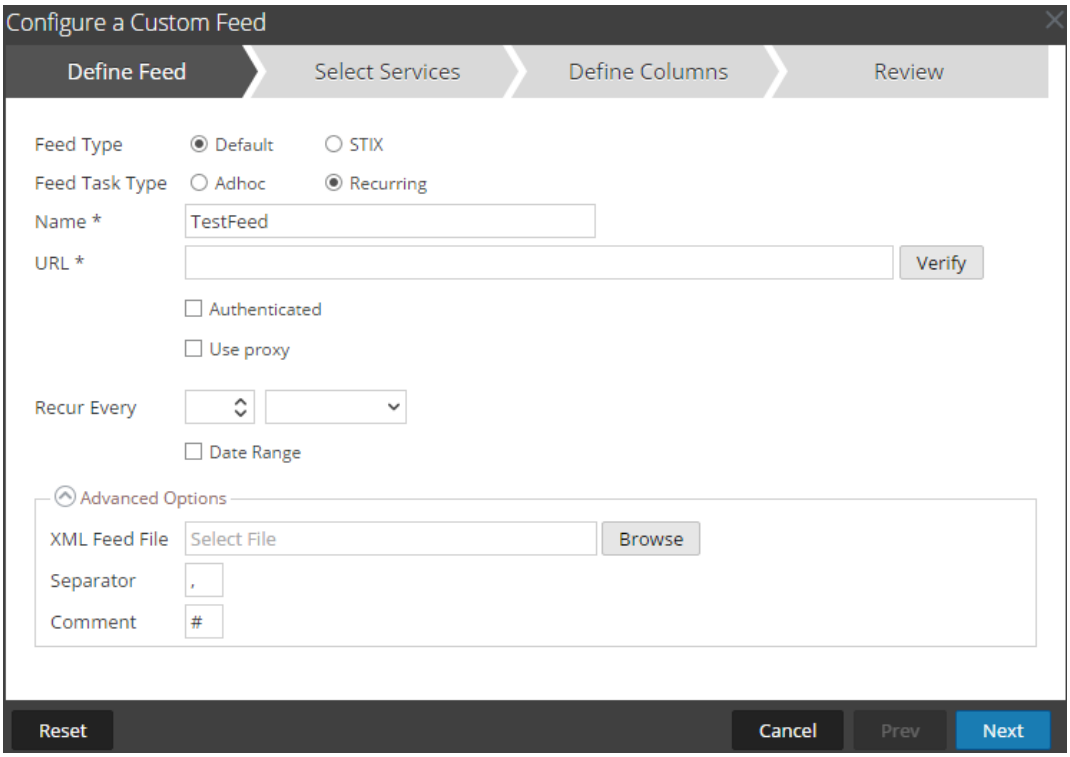
d. The Select Services form is displayed. This is an example of the form for a feed based on a feed data file with no feed definition file. If you are defining a feed based on a feed definition file, the Define Columns tab is not needed.



6. To define a recurring feed task that executes repeatedly at specified intervals, during a specified date range.

a. Select **Recurring** in the **Feed Task Type** field.

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



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

   NetWitness Suite verifiies the location where the file is stored, so that NetWitness Suite 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**.

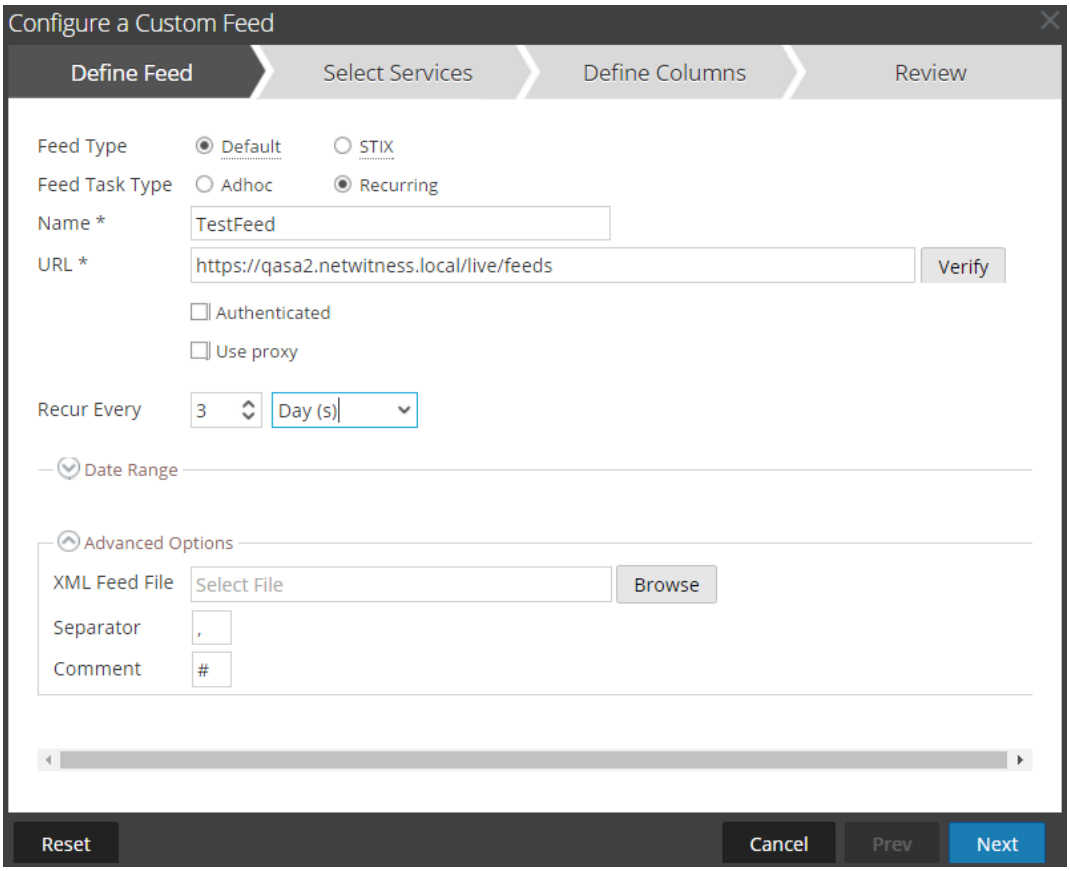
   NetWitness Suite provides your user name and password for authentication to the URL.

d. If you want the NetWitness Suite 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 Suite** topic in the *System Configuration Guide*. By default, the **Use Proxy** checkbox is not selected.

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.



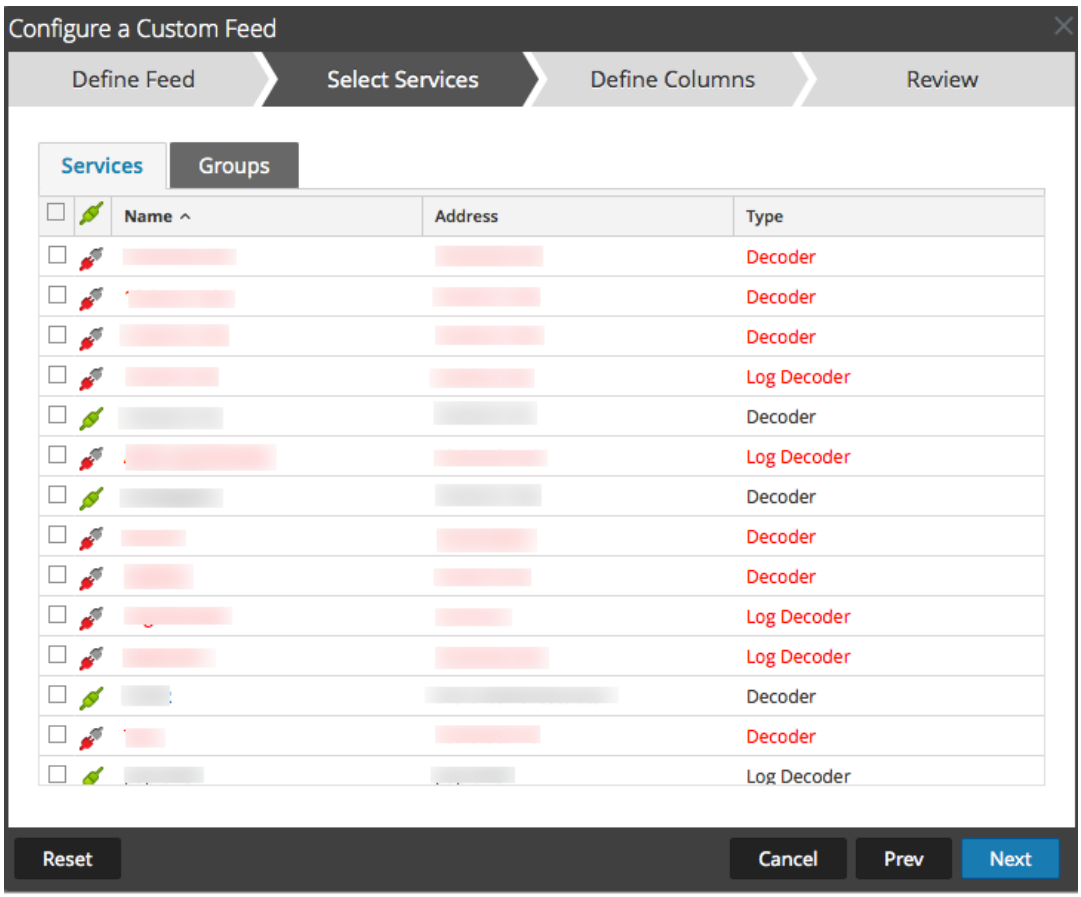
7. (Conditional) If you want to define a feed based on an XML feed file:

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

     The Advanced Options fields are displayed.

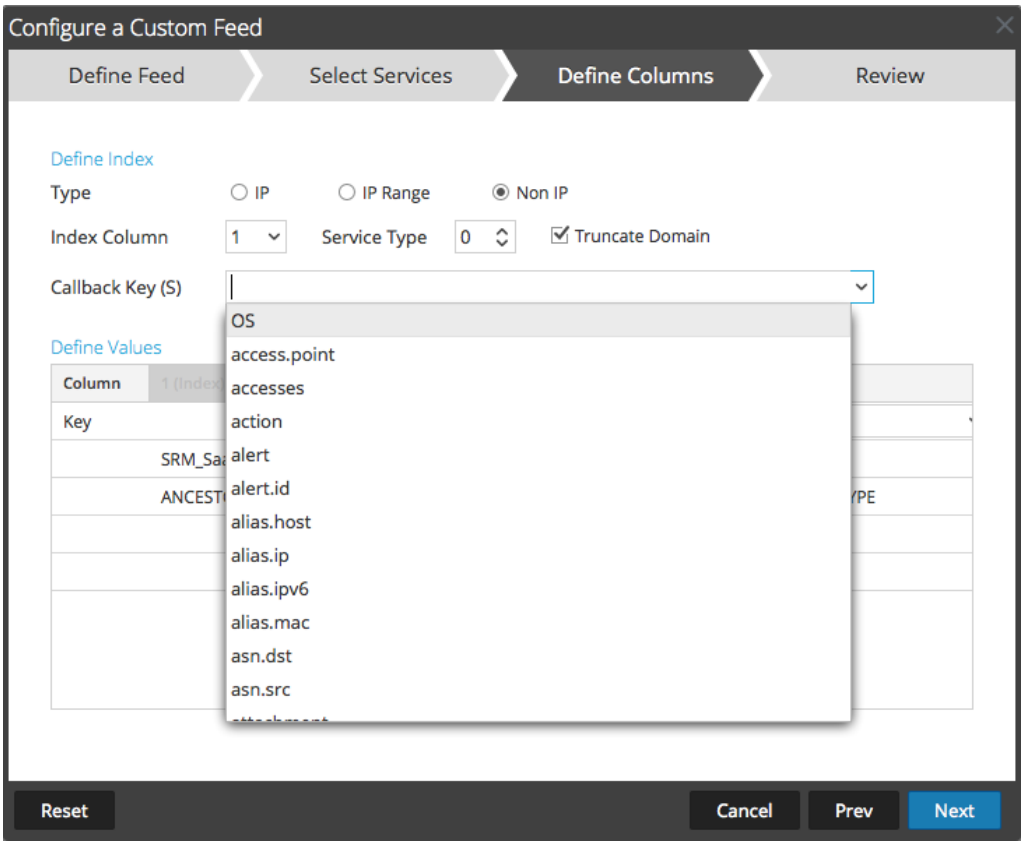
   - Select an XML feed file from the local file system, choose the **Separator** (default is comma), specify the **Comment** characters used in the feed data file (default is #) and click **Next**.

The Select Services form is displayed.

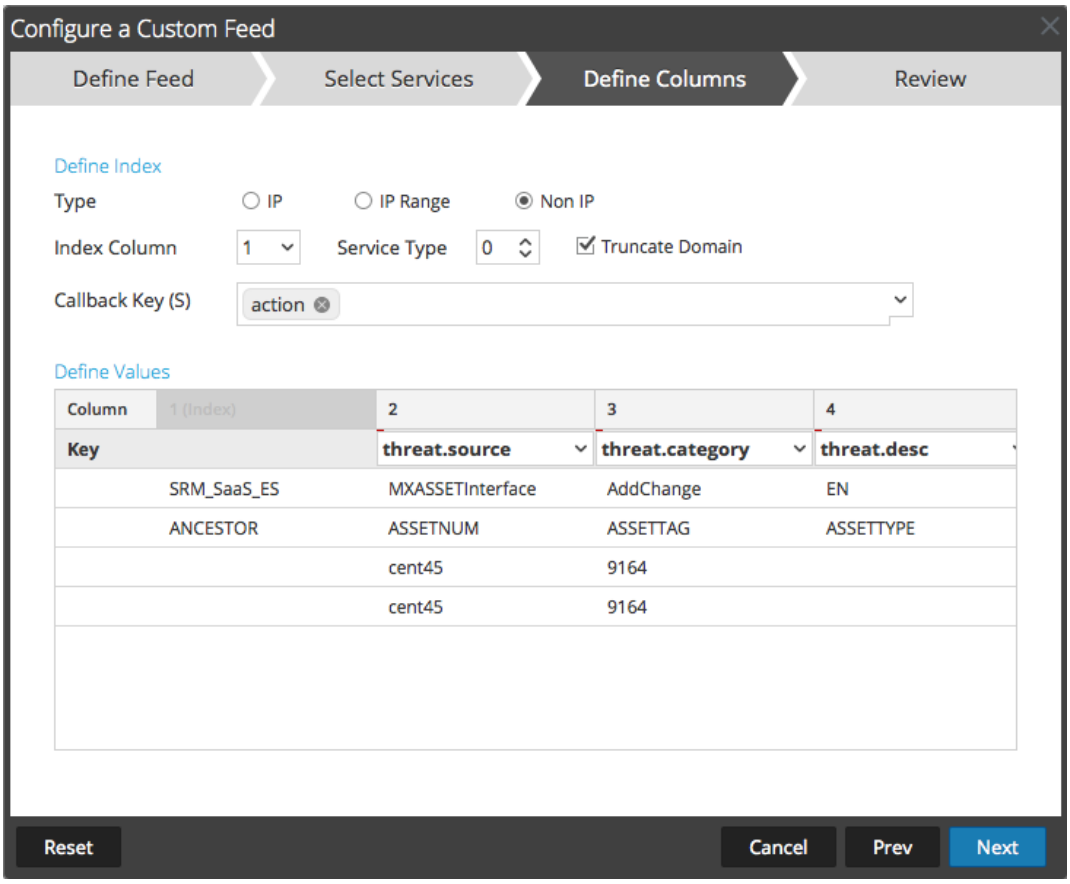


8. To identify services on which to deploy the feed, do one of the following:
   a. Select one or more Decoders and Log Decoders, and click **Next**.
   b. Click the **Groups** tab and select a group. Click **Next**.

      The Define Columns form 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** option.

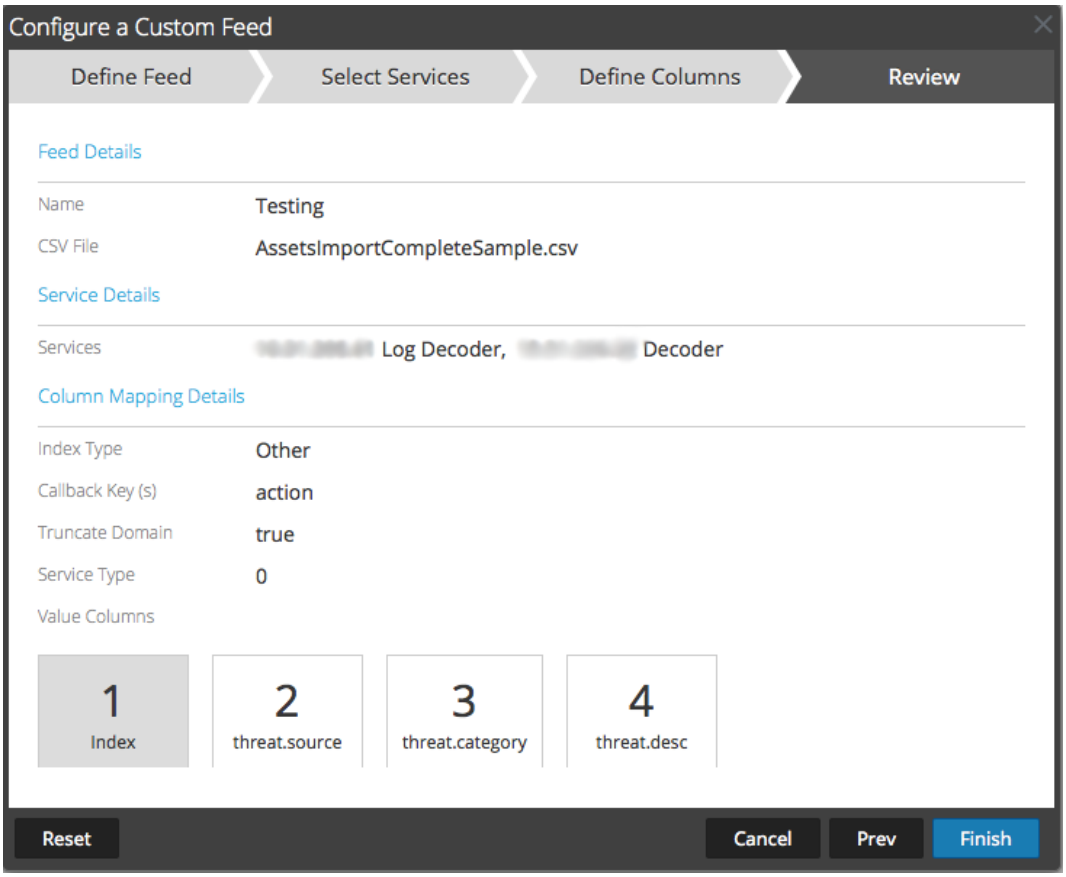


d. Select the language key to apply to the data in each column from the drop-down list. The meta displayed in the drop-down list is based on the meta available for the service define values. You can also add other meta based on advanced expertise.



e. Click **Next**.

The Review form 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.

MetaCallback Feeds using CIDR Index Range for IPv4 and IPv6

This section describes how to 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 contents of both a .csv file and an .xml file for a MetaCallback feed using CIDR index ranges for IPv4 or IPv6.

.csv file:

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

.xml 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="ip_test" path="ip_test.csv" separator="," comment="#">
        <MetaCallback name="DstIP" valuetype="IPv4" apptype="0" truncdomain="false">
                <Meta name="ip.dst"/>
        </MetaCallback>
        <LanguageKeys>
                <LanguageKey name="alert" valuetype="Text" />
        </LanguageKeys>
        <Fields>
                <Field index="1" type="index" range="cidr"/>
                <Field index="2" type="value" key="alert" />
        </Fields>
</FlatFileFeed>
</FDF>
```

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

Create a STIX Custom Feed

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

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

Note: From 10.6.1 or later, Security Analytics supports Structured Threat Information Expression (STIX).

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://stixproject.github.io/.

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

In NetWitness Suite, STIX (`.xml`) feed of type Indicator 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. And, the attributes such as Type and Title are also read from the STIX (`.xml`). The STIX (`.xml`) with a single STIX_Package is only supported.

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.

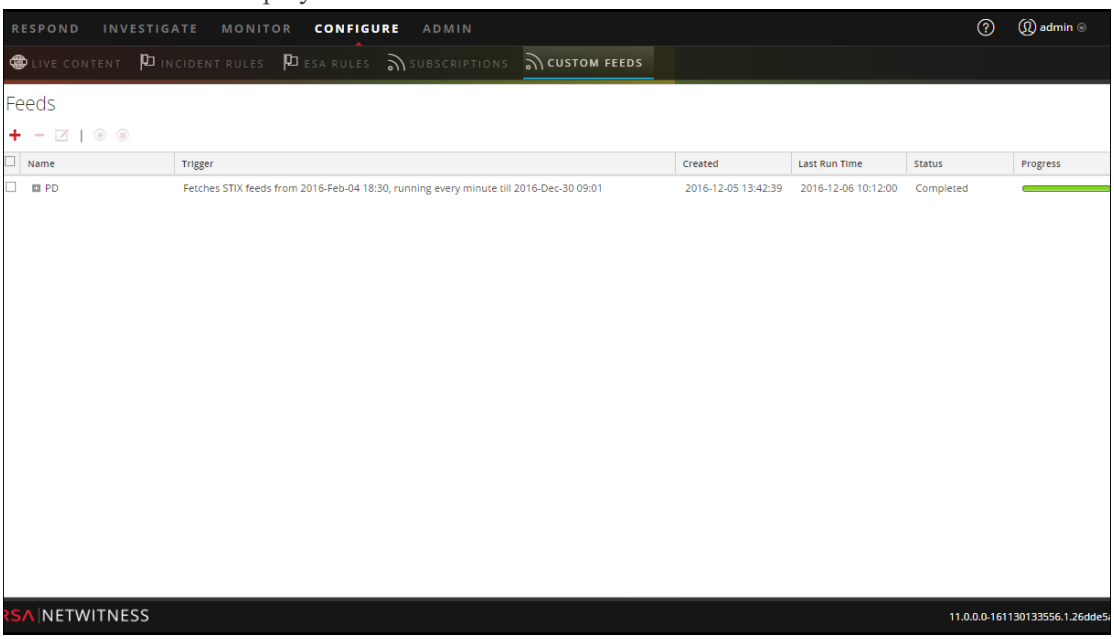
Apart from TAXII server, STIX data can also reside on REST server and you can fetch STIX file from the REST server by providing the URL of the REST server. For example, http://stixrestserver.internal.com.

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 Suite server.

To create a STIX custom feed:

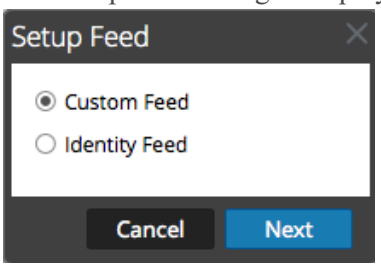
1. Go to **Configure > Custom Feeds**.

   The Feeds view is displayed.



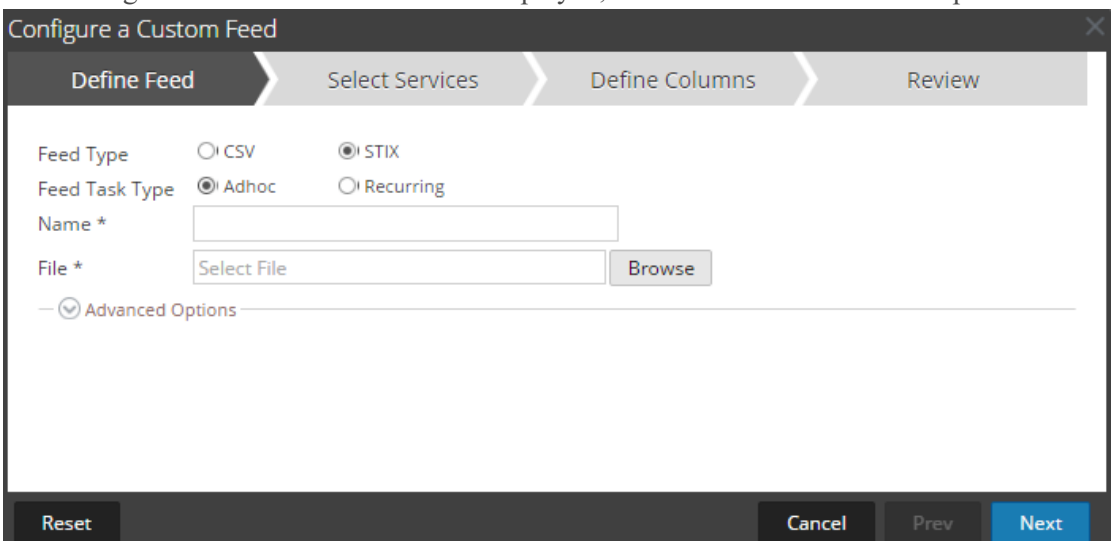
2. In the toolbar, click +.

   The Setup Feed dialog is displayed.



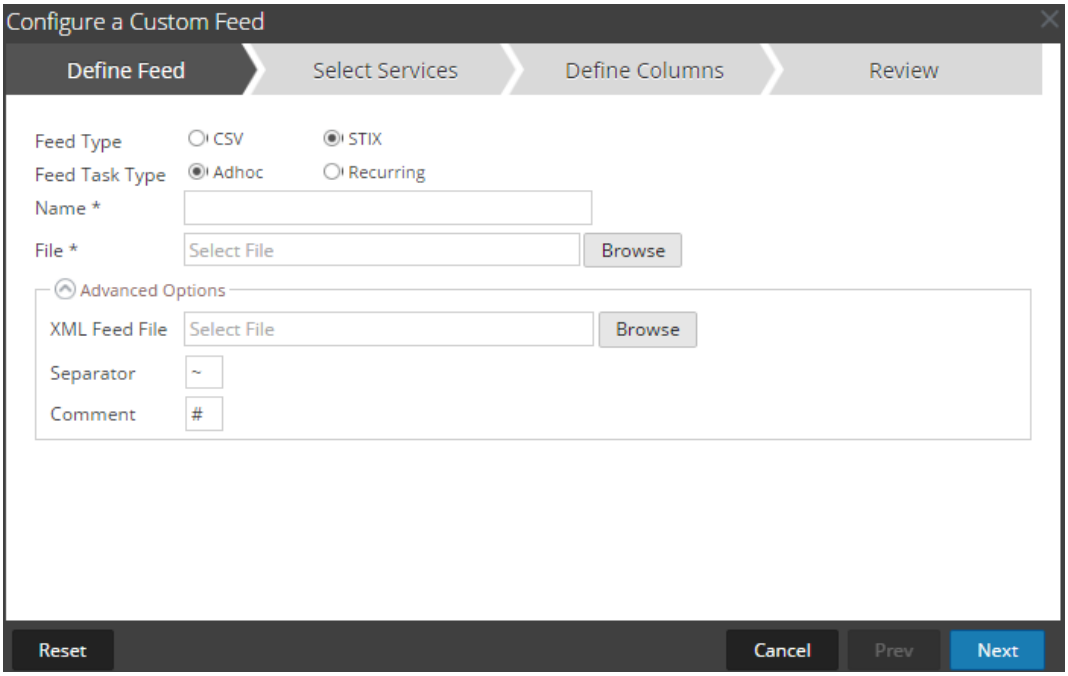
3. To select the feed type, click **Custom Feed** and **Next**.

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



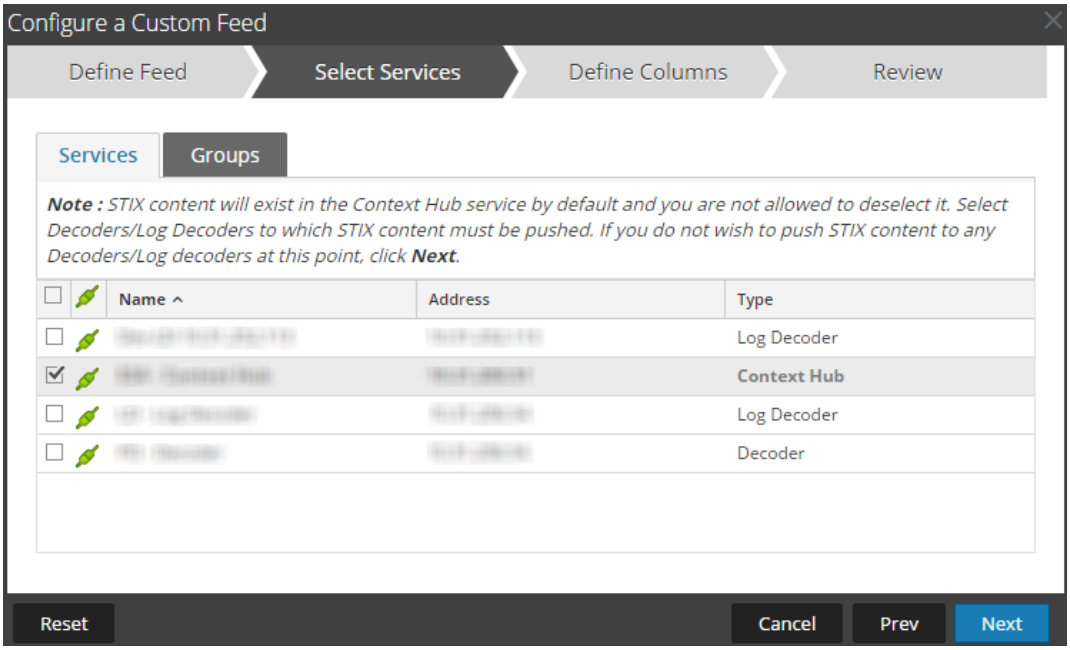
4. To define a feed based on a STIX formatted `.xml` file, select **STIX** in the **Feed Type** field.
5. To define an on-demand feed task that executes once, select **Adhoc** in the **Feed Task Type** field and do one of the following:
   a. (Conditional) To define a feed based on STIX formatted `.xml` file, type the feed **Name**, select a STIX formatted `.xml` content **File** from the local file system, and click **Next**.
   b. (Conditional) To define a feed based on an XML feed file, select **Advanced Options**.

      The Advanced Options are displayed:



c. 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**.

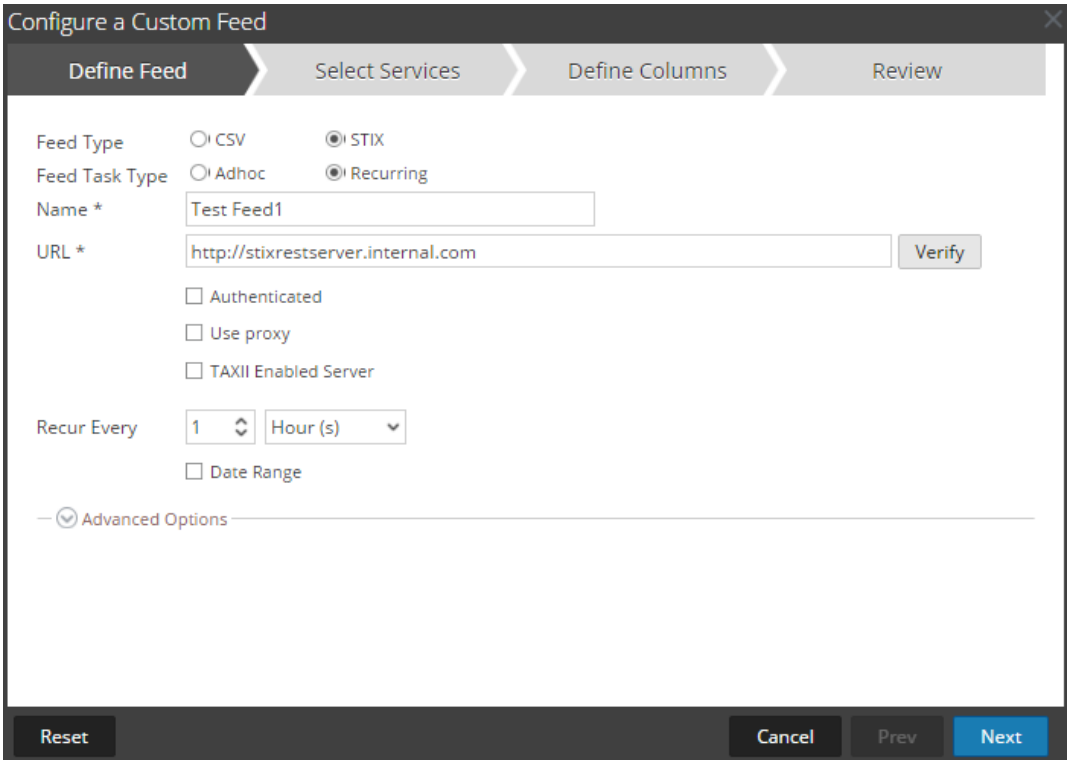
d. The Select Services form is displayed. This is an example of the form for a feed based on a feed data file with no feed definition file. If you are defining a feed based on a feed definition file, the Define Columns tab is not needed.



6. To define a recurring feed task that executes repeatedly at specified intervals, during a specified date range.

a. Select **Recurring** in the **Feed Task Type** field.

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



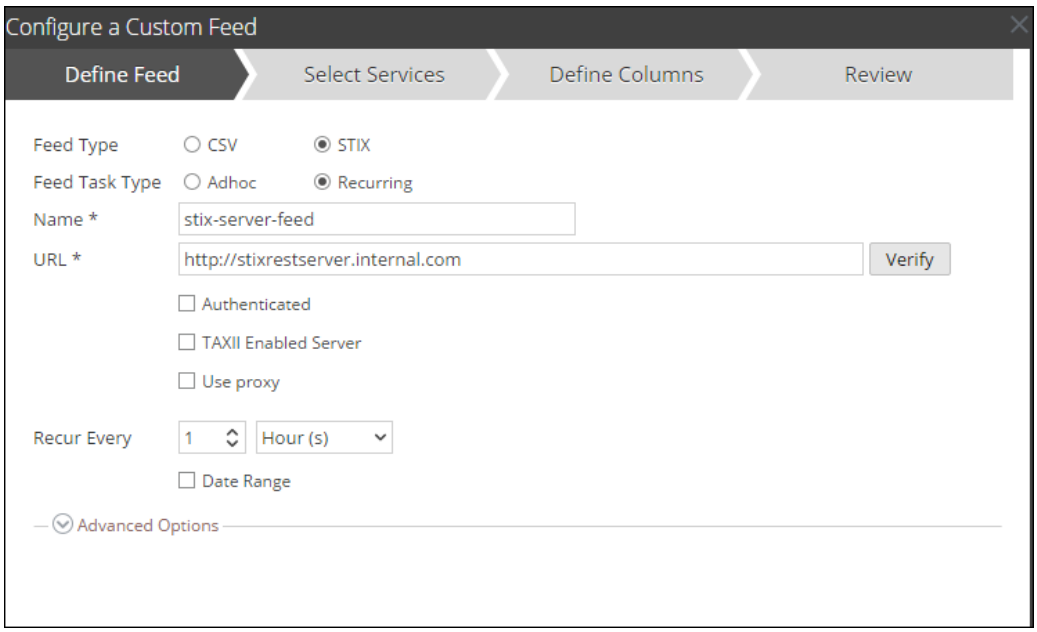
b. In the **URL** field, do one of the following:

- To define a recurring feed based on STIX which pulls STIX packages from a TAXII Server, enter the TAXII server's discovery service URL, for example, http://hailataxii.com/taxii-discovery-service.

  Note: Context Hub service installed on Event Stream Analysis host must be reachable for the specified TAXII server.

- To define a recurring feed based on a STIX formatted .xml file using REST Server, enter the URL of the REST server where the STIX data file is located, for example,

http://stixrestserver.internal.com.



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

c. If you do not want NetWitness Suite to verify the REST server's SSL certificate, Select **Trust All Certificate**. This option is enabled by default (checked)

d. For client authentication with the REST URL, in the **Certificate** field, click **Browse** and select the self signed certificate. The supported certificate formats are .cer, .crt with Base64 & DER encoded files.

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

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

f. Select **TAXII Enabled Server**, if you want to select a TAXII collection from the list. For a valid URL, one or more TAXII collections that contains the STIX data file is displayed based on your credentials. Select the required TAXII collection from the list. Only one collection can be added from a TAXII server for a feed.

Note: Though multiple feeds from multiple TAXII servers are supported, only one account (username and password) is supported per TAXII server.

g. If you want the NetWitness Suite 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 Suite topic in the *System Configuration Guide*. By default, the **Use Proxy** checkbox is not selected.

h. (Optional) Click **Verify** to test the settings.

Note: Make sure all the required connection parameters such Authentication, Proxy, Certificate trust, TAXII Enabled Server etc. are configured before you click **Verify**.

i. To define the interval of recurrence for pushing to Decoder or Log Decoder, 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.

j. 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 Start Date should be defined from when you want to fetch the data. Make sure that the **Start Date** is not before 180 days from today.

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

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

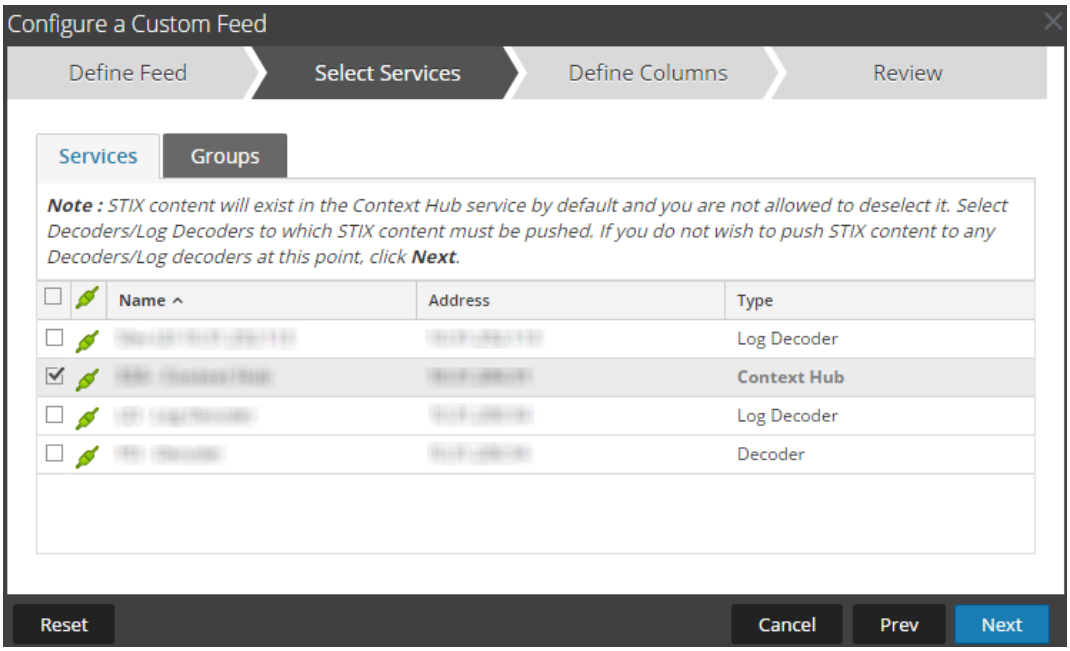
  The Advanced Options fields are displayed.
- Select an XML feed file from the local file system, choose the **Separator** (default is comma), specify the **Comment** characters used in the feed data file (default is #).
- In the **Remove STIX data older than** field, specify the number of days for which STIX packages pulled from TAXII server is to be stored. The STIX packages older than the specified number of days is deleted automatically.
- Click **Next**.

  The Select Services form is displayed.

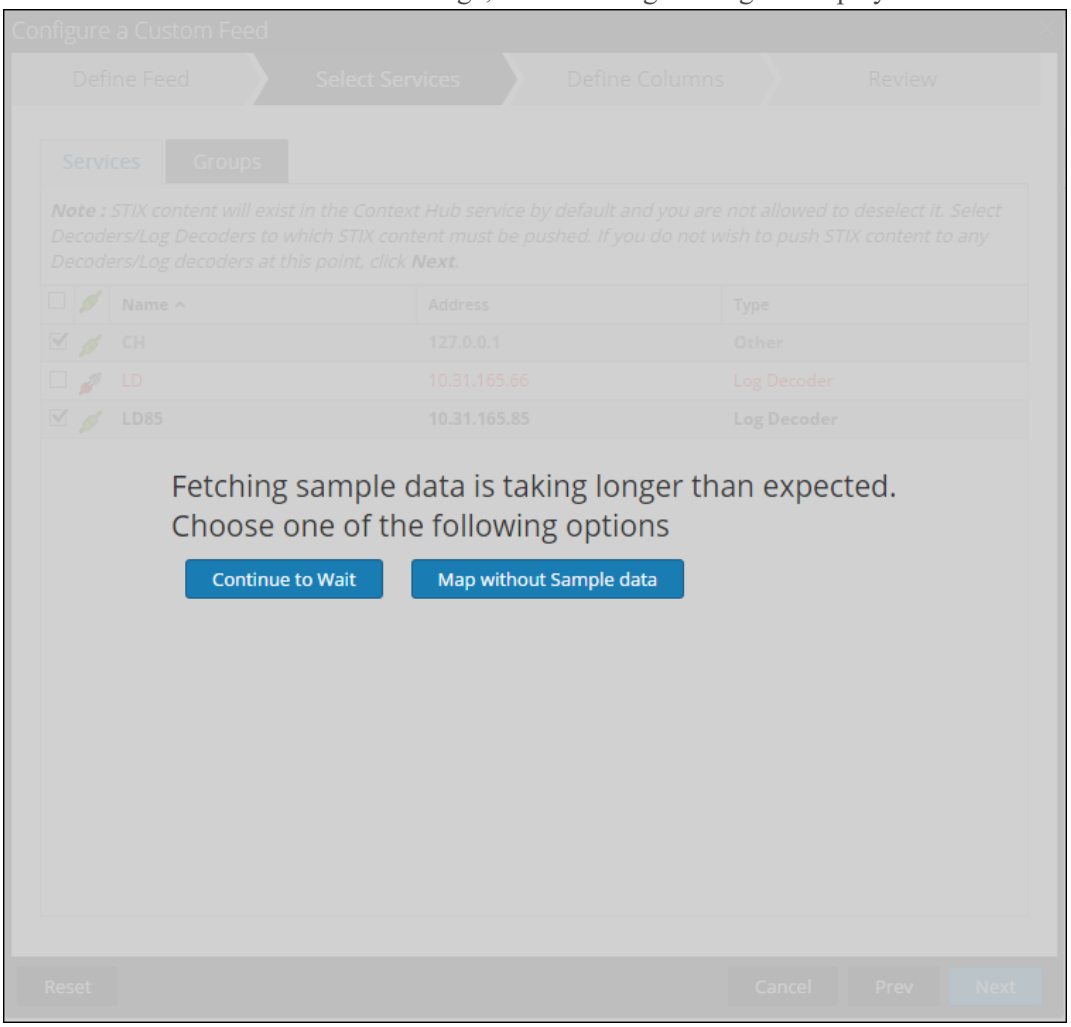
8. To identify services on which to deploy the feed, do one of the following:

a. Select one or more Decoders and Log Decoders, and click **Next**.

b. 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**.


Configure a Custom Feed
Define Feed
Select Services
Define Columns
Review
Services
Groups
Note : STIX content will exist in the Context Hub service by default and you are not allowed to deselect it. Select Decoders/Log Decoders to which STIX content must be pushed. If you do not wish to push STIX content to any Decoders/Log decoders at this point, click Next.
Name
Address
Type
Log Decoder
Context Hub
Log Decoder
Decoder
Reset
Cancel
Prev
Next

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

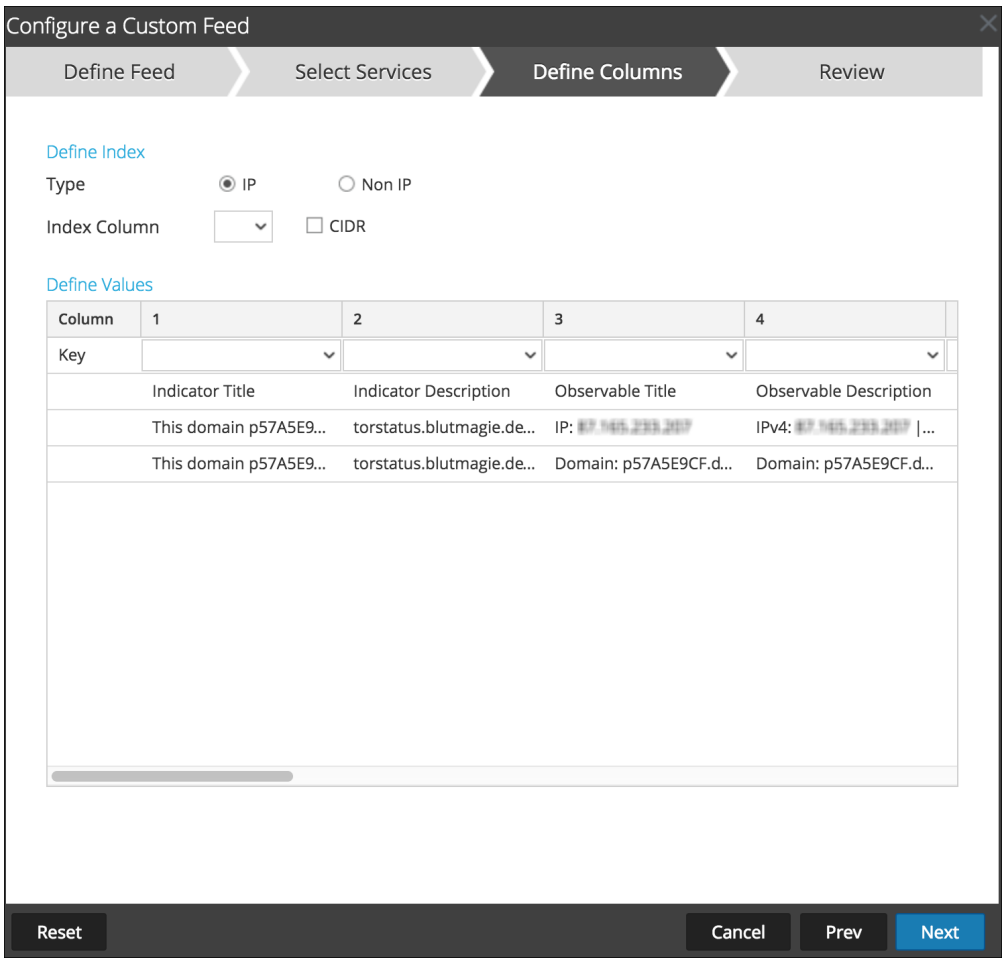


- If you click **Continue to Wait**, it continues to wait till the sample data is fetched or timeout (10 minutes) whichever is sooner. In case of timeout no sample data is retrieved even after 10 minutes.
- If you click **Map Without Sample data**, the mapping column is displayed without any sample data.

The Define Columns form 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** option.

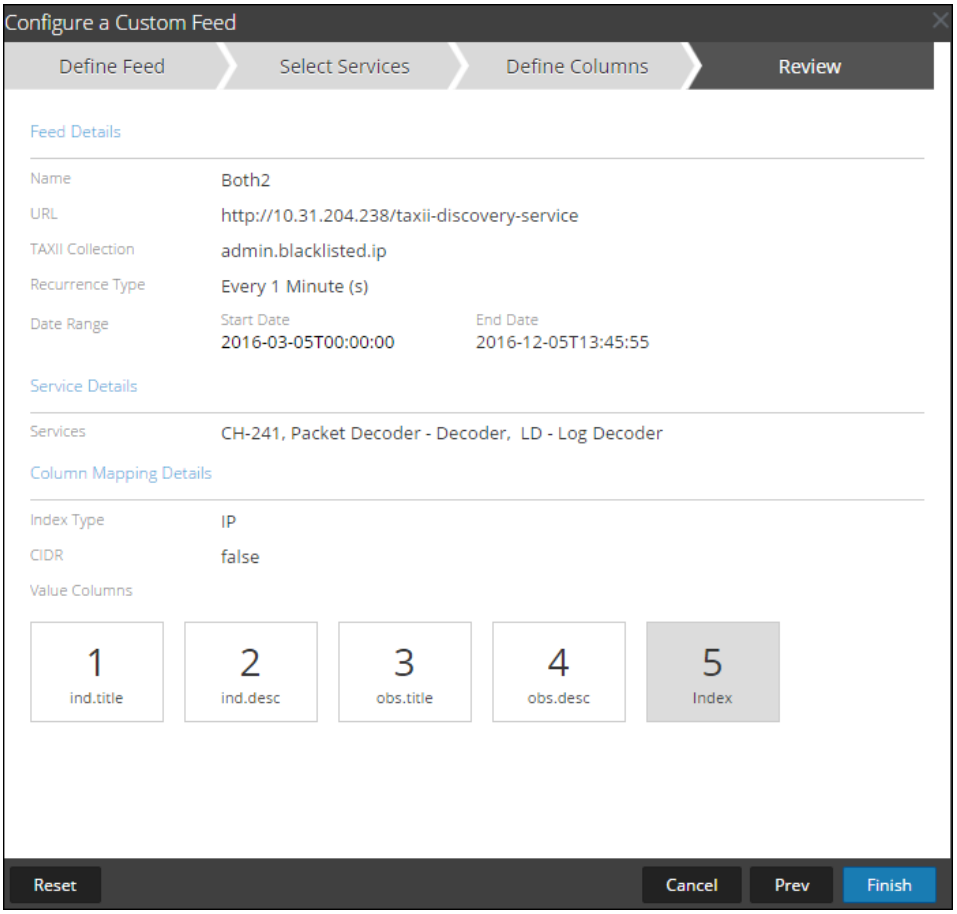


Note:
- If the **Index Type** is Non IP, you can select multiple index columns in the **Index Column(S)**. The values from all the selected columns are merged in the first index column that you selected and the merged values are pushed to the Log Decoder for parsing. For example, in the **Index Column(S)** 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.

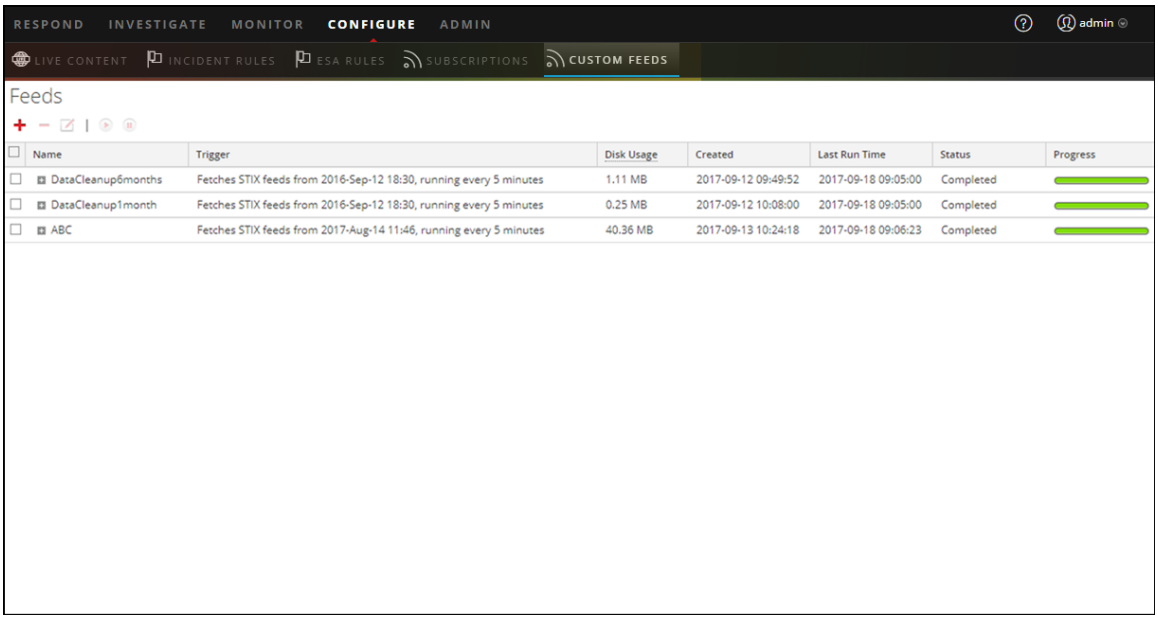
e. Click **Next**.

The Review form 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: 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 due to low memory. For more information on how to troubleshoot `OutOfMemoryError` on `Contexthub` Server, refer to "Troubleshooting" in the *Live Services Management Guide*.

MetaCallback Feeds using CIDR Index Range for IPv4 and IPv6

This section describes how to 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 contents of both a .csv file and an .xml file for a MetaCallback feed using CIDR index ranges for IPv4 or IPv6.

.csv file:

192.168.0.0/24, Sydney
192.168.1.0/24, Melbourne

.xml 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="ip_test" path="ip_test.csv" separator="," comment="#">

        <MetaCallback name="DstIP" valuetype="IPv4" apptype="0" truncdomain="false">

                <Meta name="ip.dst"/>
```

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

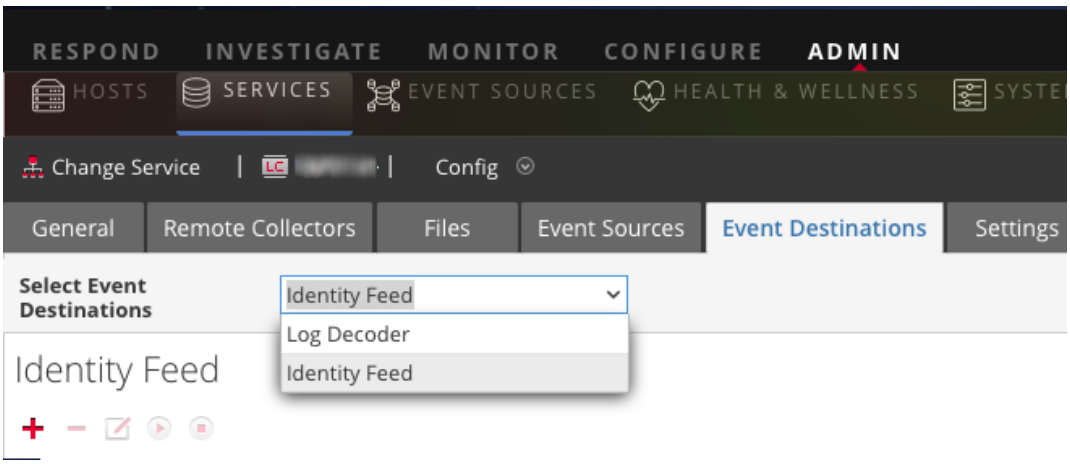
Note: To configure a CIDR index range for feeds with single or multiple MetaCallbacks of value type IPv4 or IPv6, the field of type index MUST contain a range attribute with range="cidr". Also, configuring "cidr" index ranges for feeds with MetaCallbacks of multiple different value types is not supported.

Create and Manage 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.

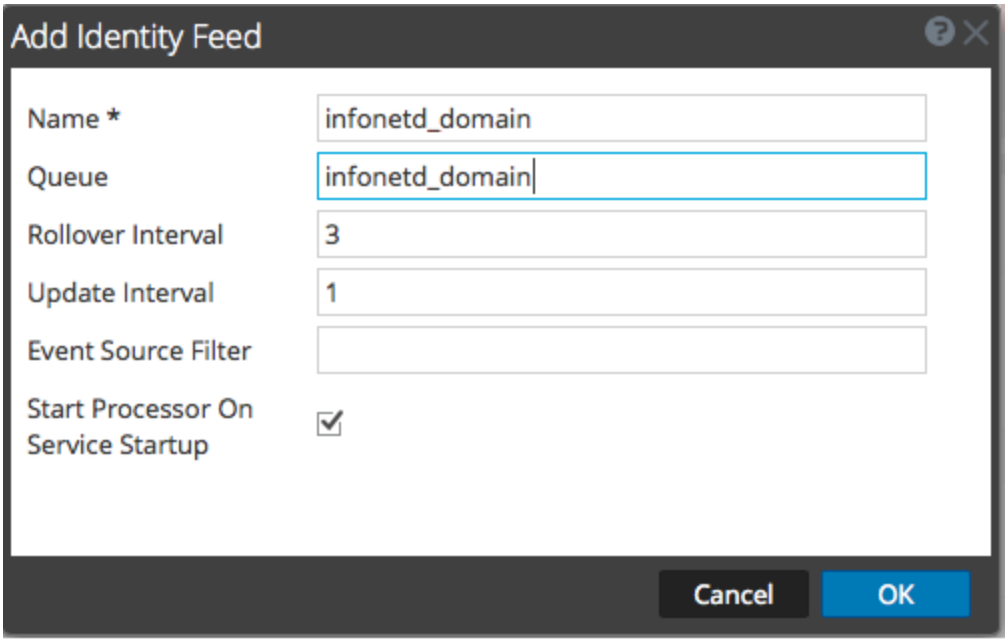
To create an identity feed:

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



d. 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.

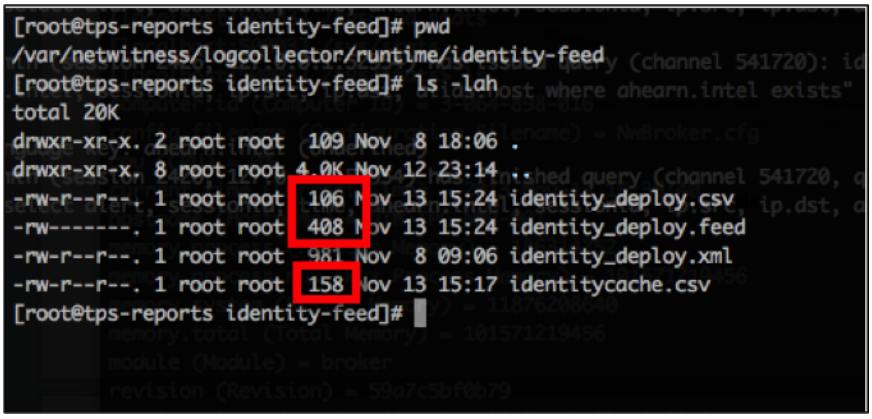


e. Click **OK**.

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.

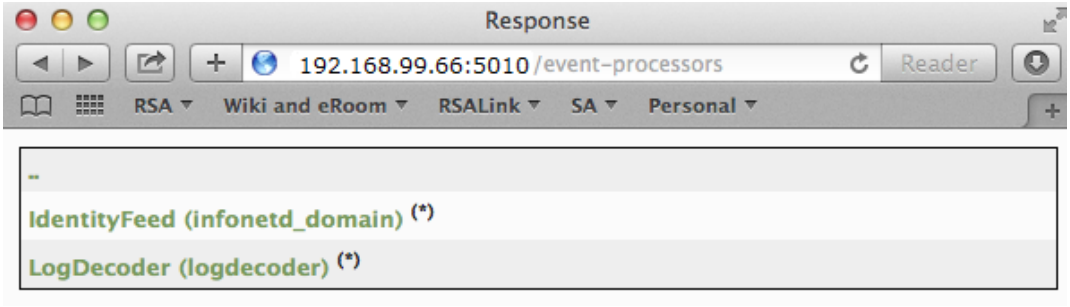
b. Verify that data is written to the feed files. SSH to the Log Decoder/Collector or Virtual Log Collector being configured. Navigate to `/var/netwitness/logcollector/runtime/identity-feed` and verify that the `Identity_deploy` files are getting populated with data.



c. Open up a web browser (Non-Internet Explore 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:

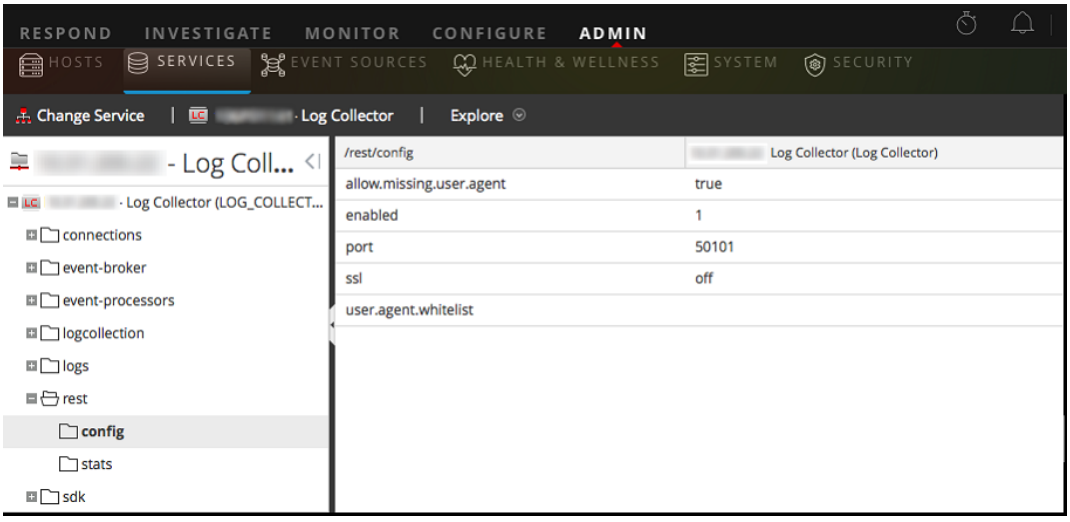


Notice the screen contains the name of the identity feed you created earlier (`infonetd_domain`, in this example).

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**.



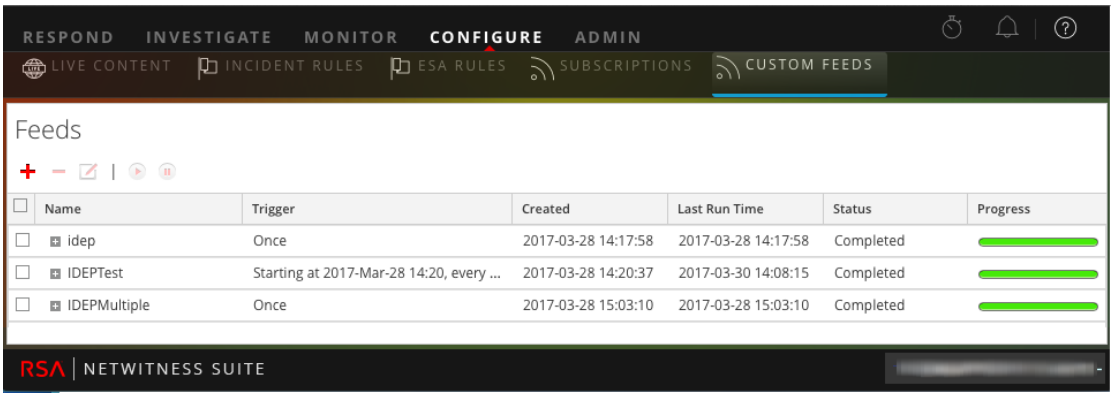
For REST to be active, **enabled** must be set to **1**.

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.

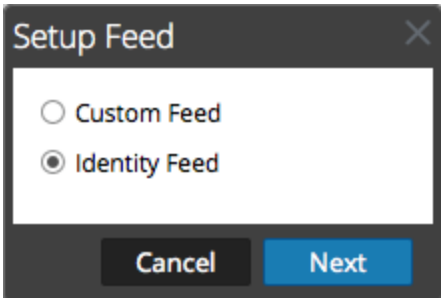
3. Go to **CONFIGURE > Live Content > Custom Feeds**.

   The Feeds grid is displayed.



4. In the toolbar, click +.

   The Setup Feed dialog is displayed.



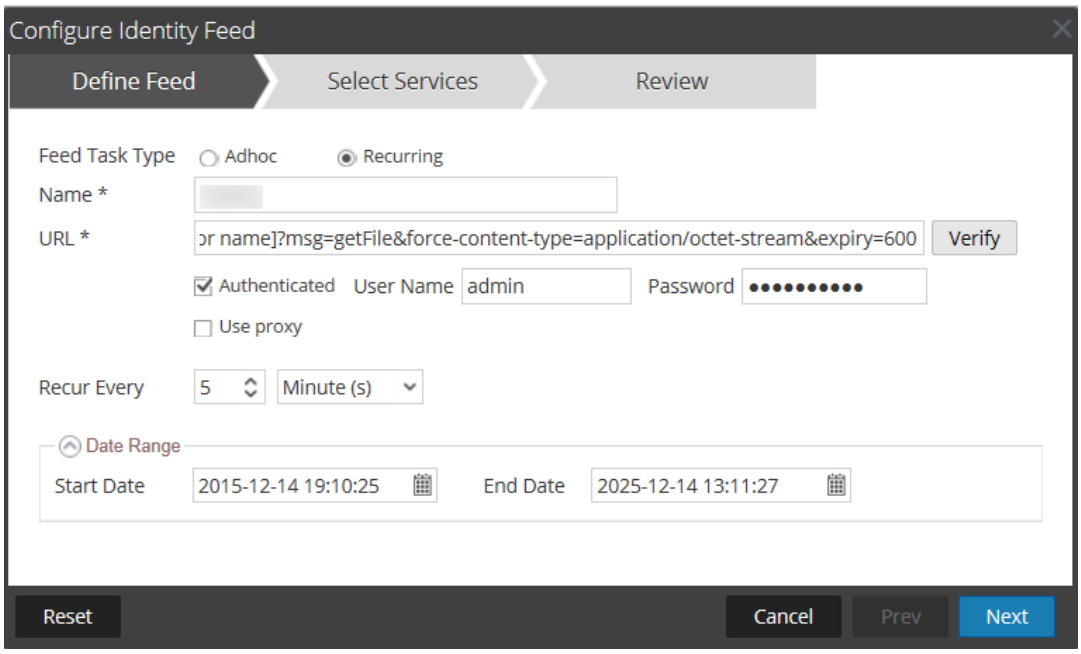
5. Ensure **Identity Feed** is selected and click **Next**.

   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** form includes the fields for a recurring feed.



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

7. Fill in 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. You need to know 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 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 our 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 Security Analytics UI server can access the log collector's REST API port (50101). This can be tested by going to the Security Analytics 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 Security Analytics UI server and the Log Collector.

Example of 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 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 details, 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 Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.)

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

   - Specify the number of minutes, hours, or days between recurrences of the feed.
   - 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.

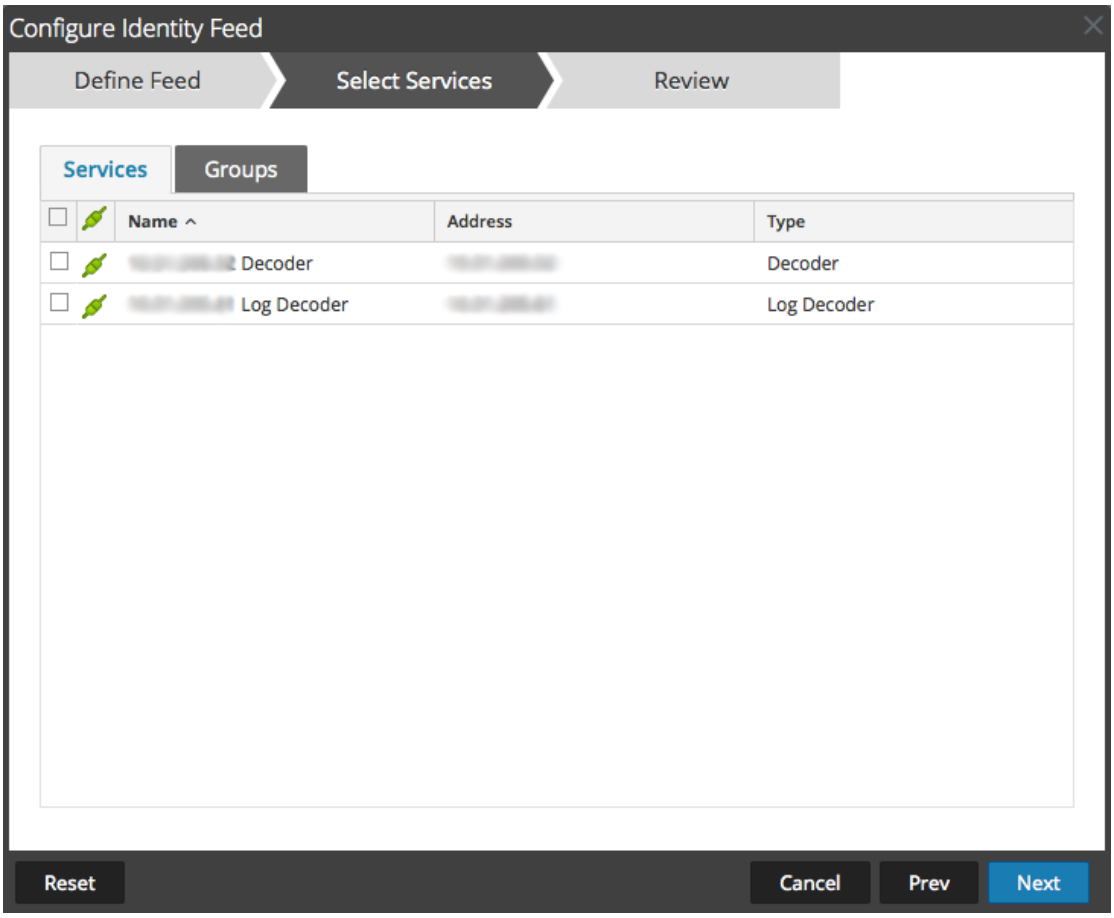
10. If using SSL encryption, you need to install the REST API SSL certificate for the log Collector into the Security Analytics UI server. For details, see Import the SSL Certificate.

    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 form.

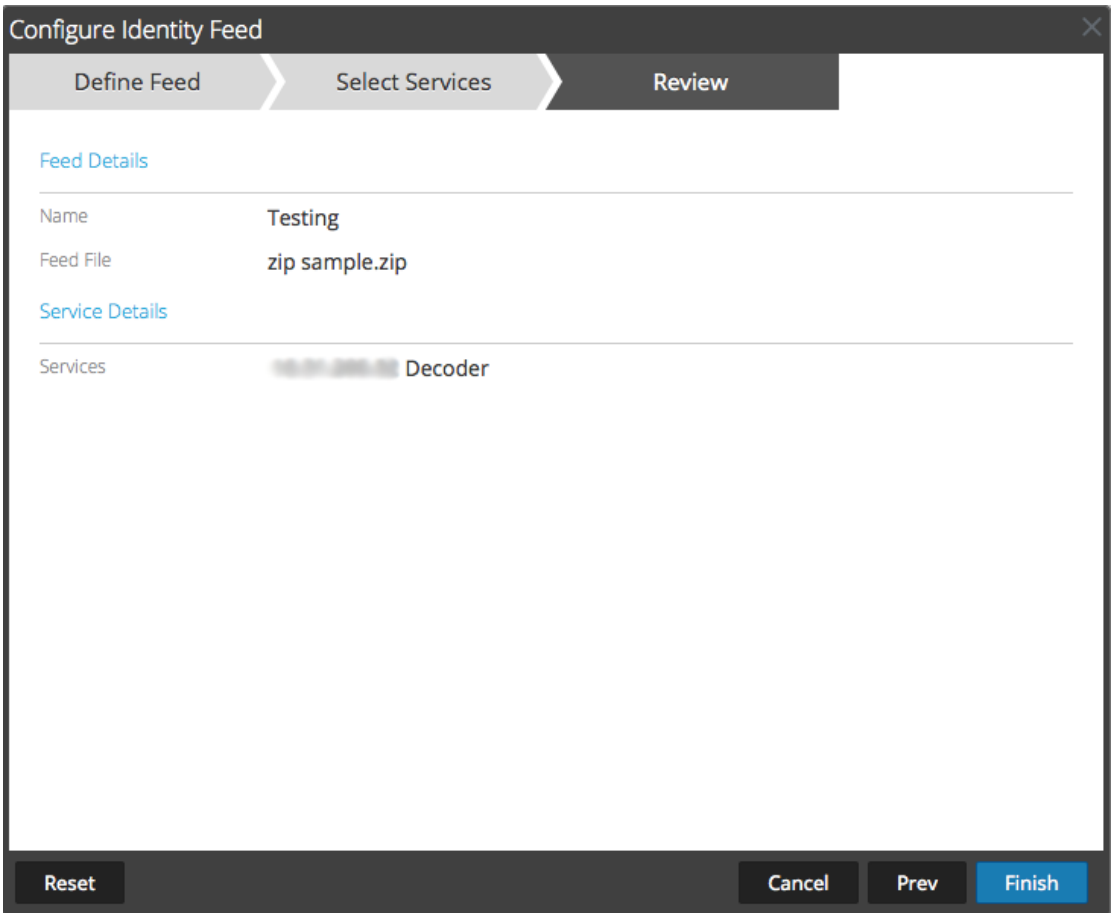
12. Click **Next**.

    The Select Services form is displayed.



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

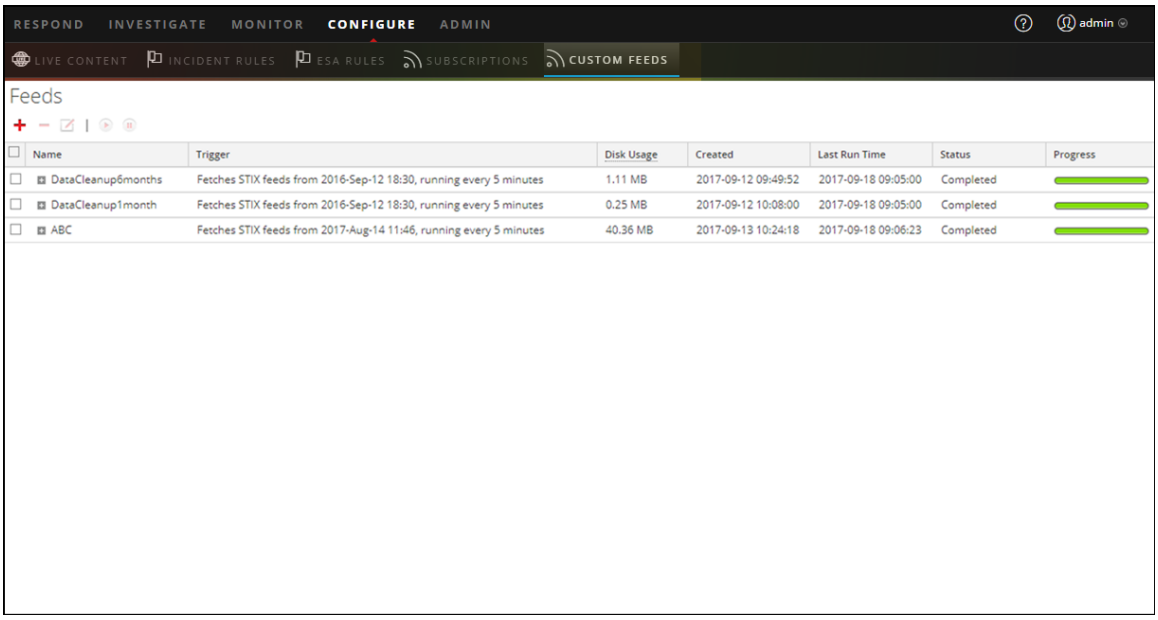
    The Review form is displayed.



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.



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 Security Analytics UI server key store. If this certificate is not imported, the Security Analytics 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 Security Analytics 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 Security Analytics 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 Security Analytics 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 still 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.

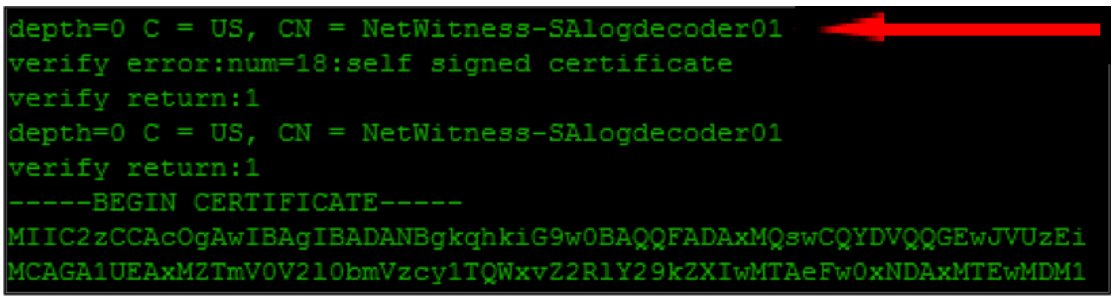
1. SSH to the Security Analytics UI server.
2. Run the following command to output the CN name of the SSL cert:

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

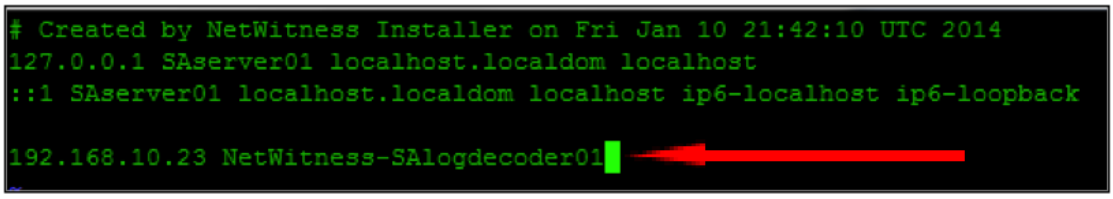
   Example:

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

3. Retrieve the CN name of the SSL certificate.



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



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.

Investigate 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/non-Domain Controller is configured. Note that identity feeds can only be processed via an Identity Feed Event Processor.

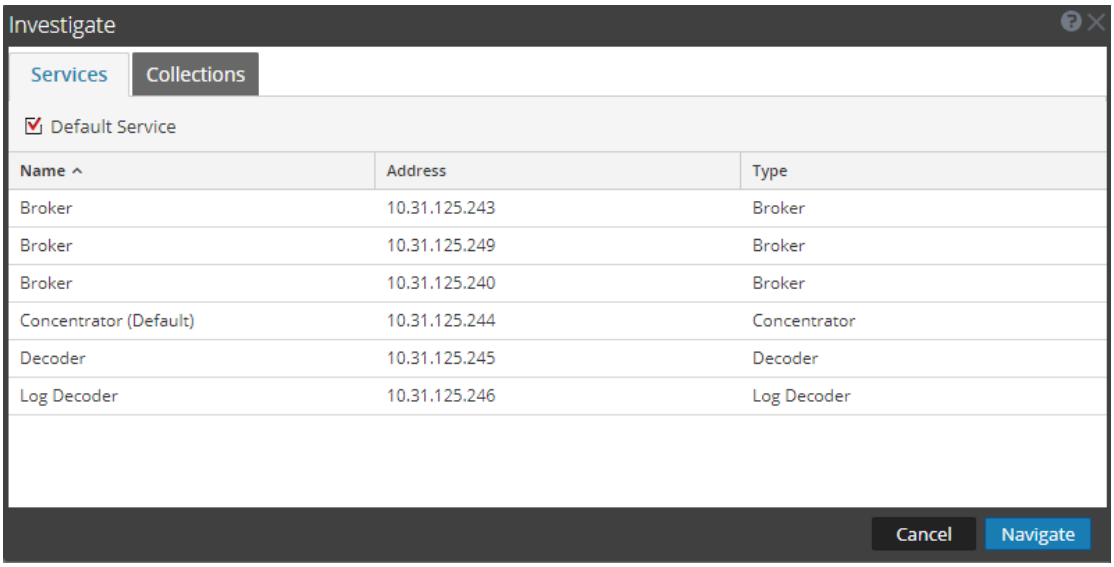
Note: An identity feed only tracks one log in at a time. If two users log in to a system at the same time, the second user will overwrite the first user's data in the identity feed.

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

To investigate a configured identity feed:

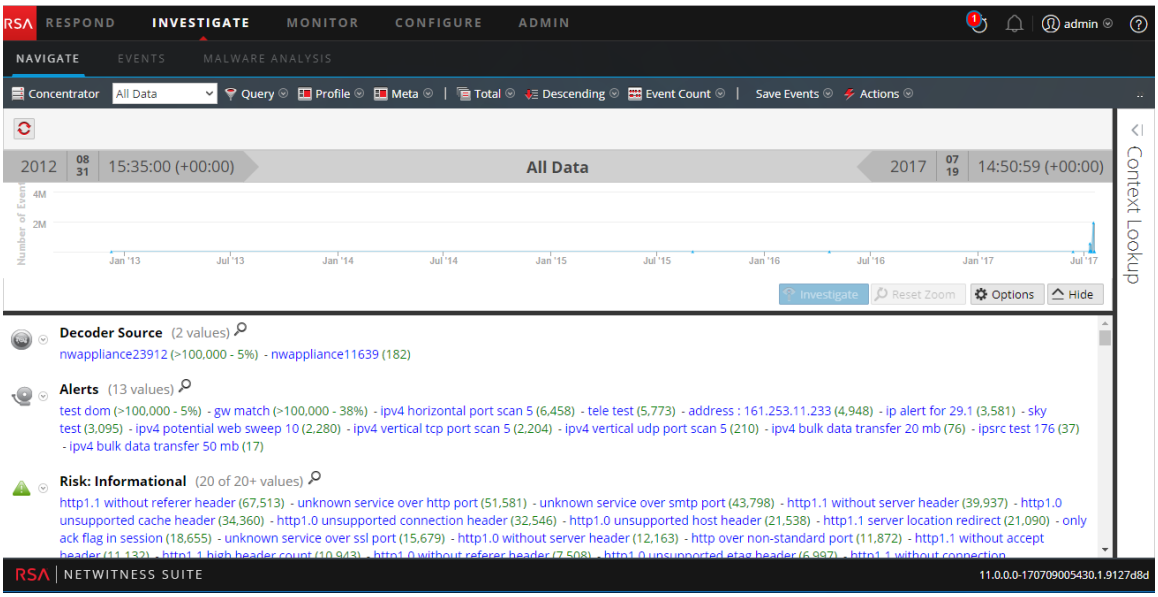
1. Go to **INVESTIGATE > Navigate**.

   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 shown in the following illustration.



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.

Edit a Feed

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

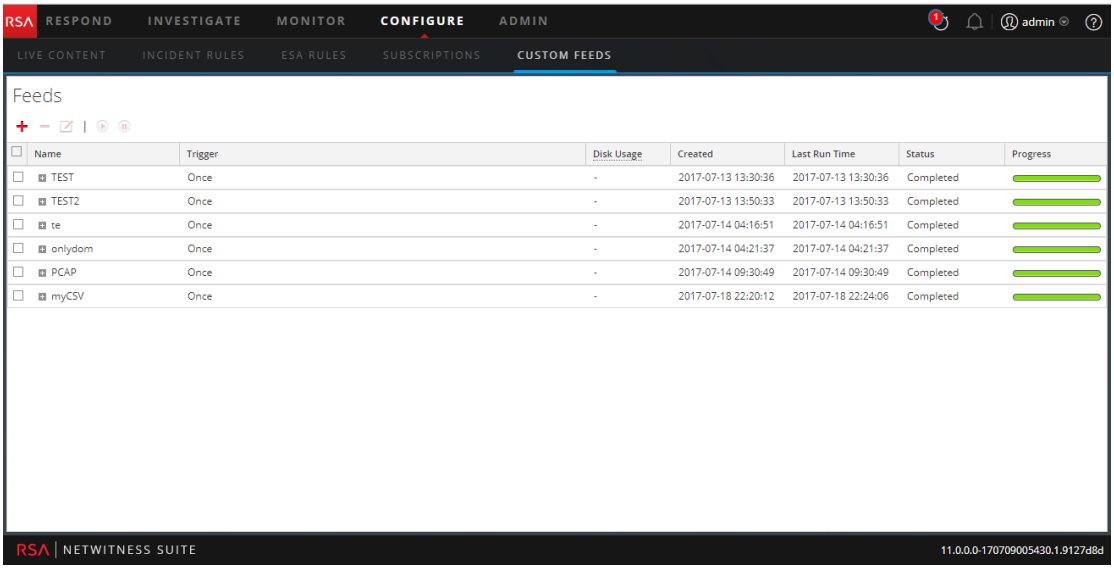
Completing this procure will result in:

- An existing custom feed opened.
- The feed (**.zip** format) or the file used to create the feed (**.csv** or **.xml**) downloaded and edited.
- The feed recreated with the updated file and new feed specifications.

To edit an existing feed:

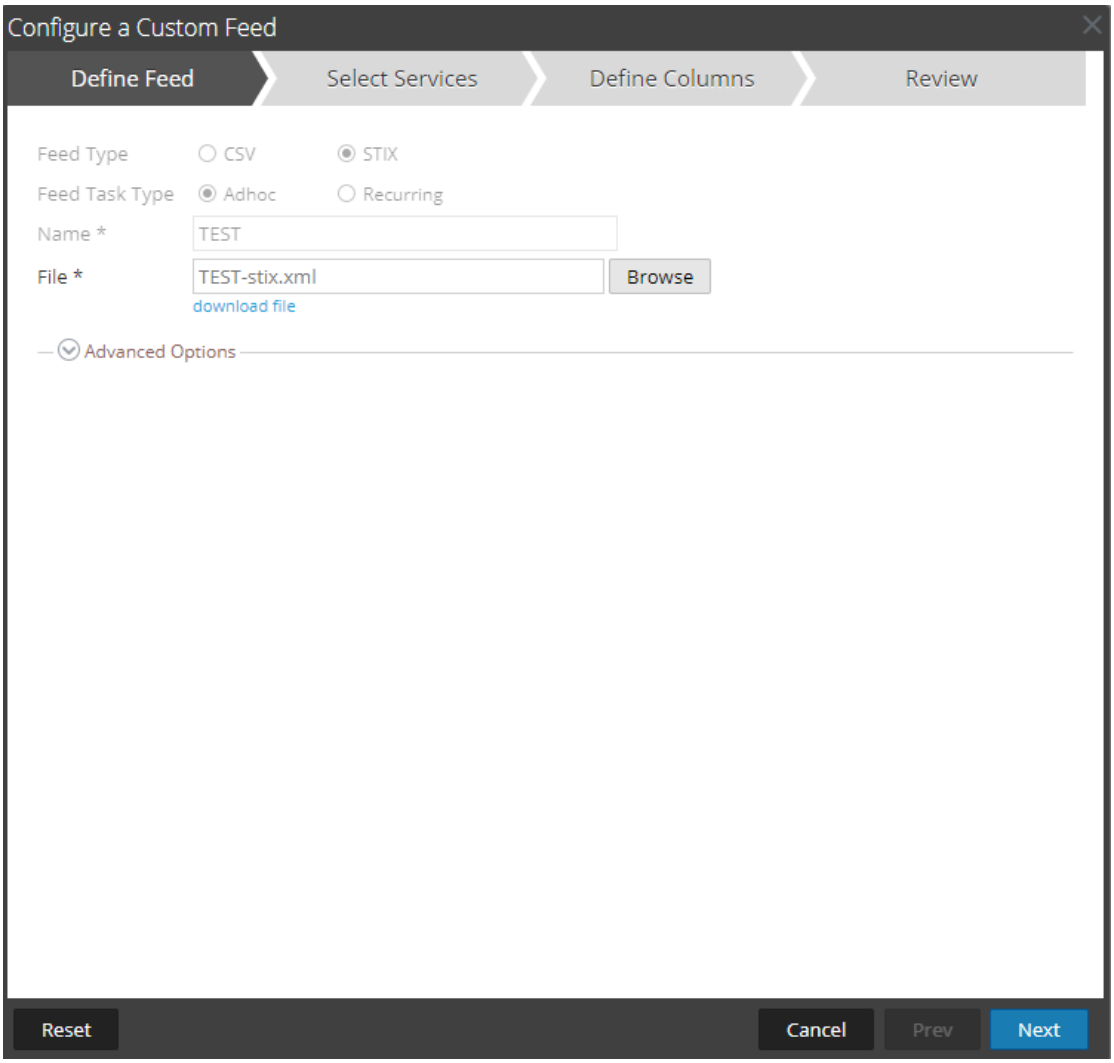
1. Go to **CONFIGURE > CUSTOM FEEDS**.

   The Custom Feeds view is displayed.



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

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



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 form (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.

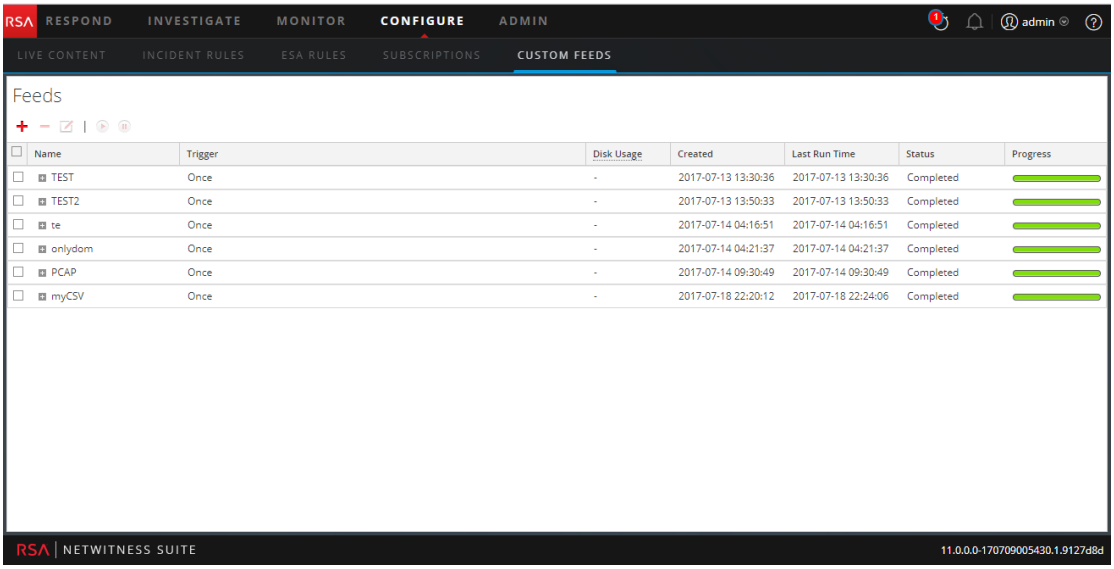
Remove a Feed

This topic provides instructions for removing a feed.

To remove a feed:

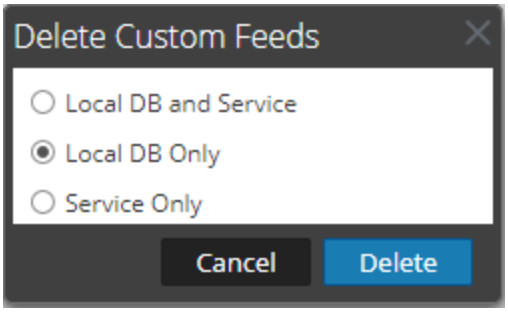
1. Go to **CONFIGURE > CUSTOM FEEDS**.

   The Custom Feeds view is displayed.



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

   The Delete Custom Feeds dialog is displayed.



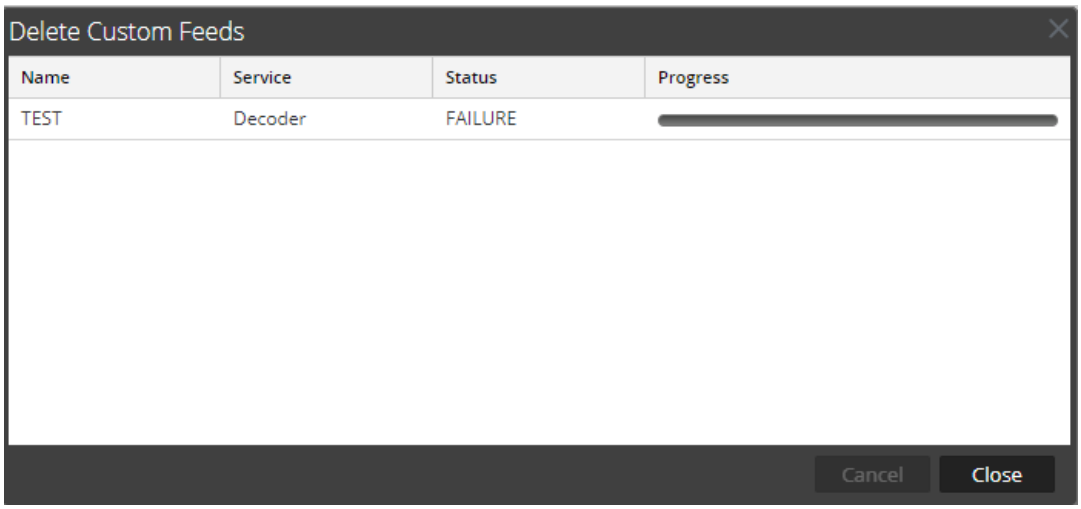
You can select one of the following options to delete the feed:

- If you choose to delete the feed from **Local DB and Service**, the feed is deleted from both the service and the local NetWitness Suite box. The deleted feed will no longer seen on the NetWitness Suite user interface.
- If you choose to delete the feed from **Local DB Only**, the feed is deleted from the local NetWitness Suite box. The deleted feed will not be seen on the NetWitness Suite 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 Suite user interface and can be deployed again

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

   A warning dialog is displayed.

4. Click **yes** to confirm that you want to delete the feed from the select areas.
   - If you chose to delete the feed from the **Local DB Only**, the feed is deleted.
   - If you chose to delete the feed from the **Local DB and Service** or **Service Only**, the Delete Custom Feeds view is displayed showing the progress of the deletion on the service.



Miscellaneous Live Services Procedures

This section covers the following procedures:

Add Subscribed Resources for Deployment to Services

1. Navigate to the **CONFIGURE > SUBSCRIPTIONS > Deployments Tab**.
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.

Delete 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 Suite Live.

To delete a subscription:

1. In the **Subscriptions tab**, select the subscriptions that you want to delete.
2. Click .

   A dialog asks for confirmation that you want to delete the subscription.
3. To confirm removal, click **Yes**.

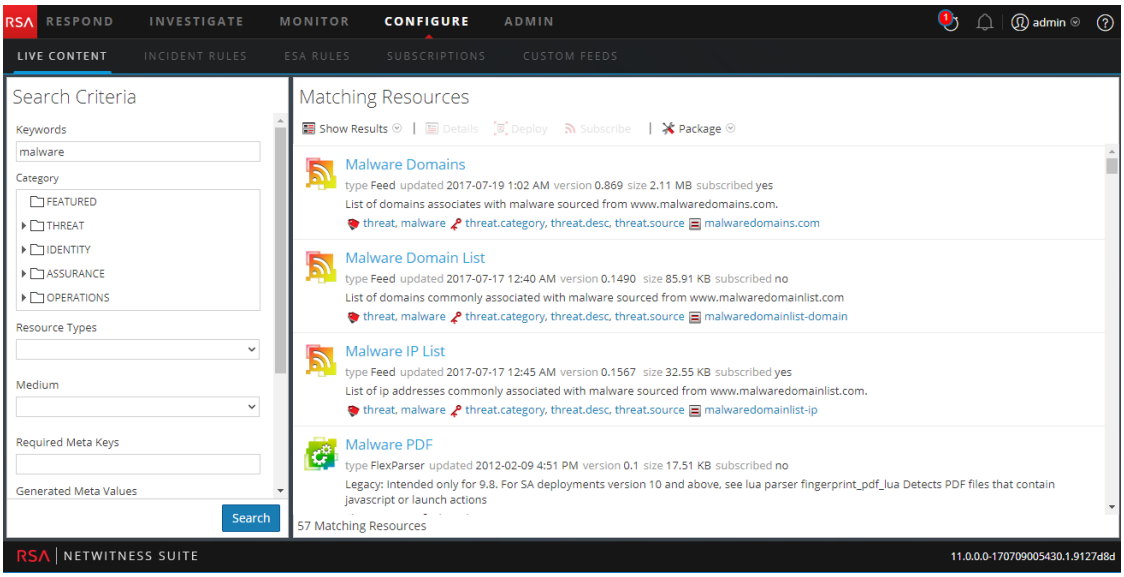
   The subscription is deleted from the subscriptions list, but any deployed instances of the subscribed resource remain on the services.

Display Resource Details in Live Resource View

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

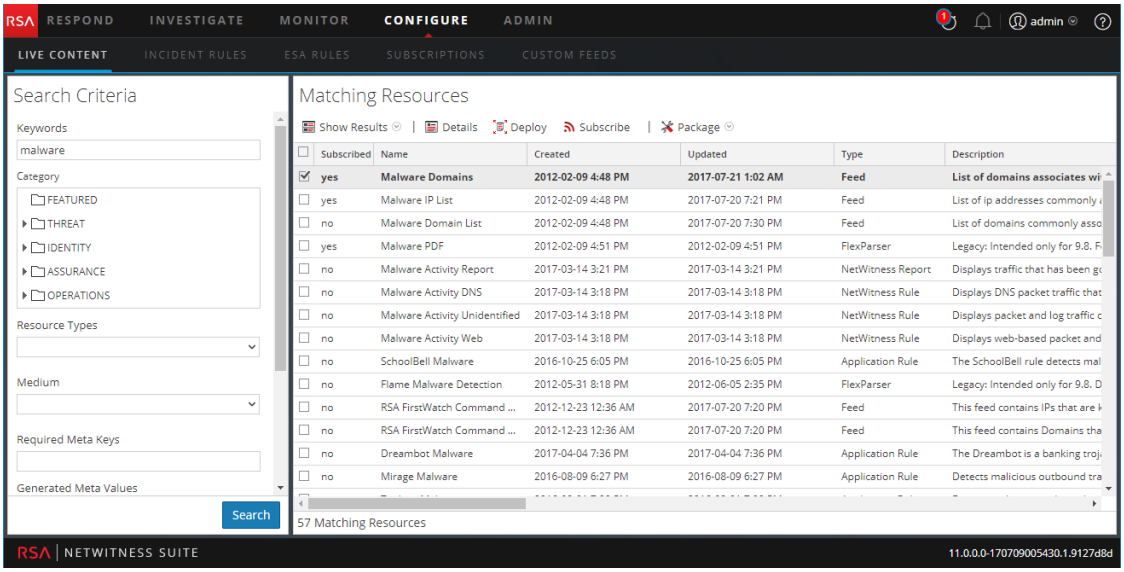
To open a separate tab in the Live Resource view with details of a selected resource, do one of the following:

- If you are viewing the **Detailed Results**, click the resource type icon or the resource name.



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

Details.



Download 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 that 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.

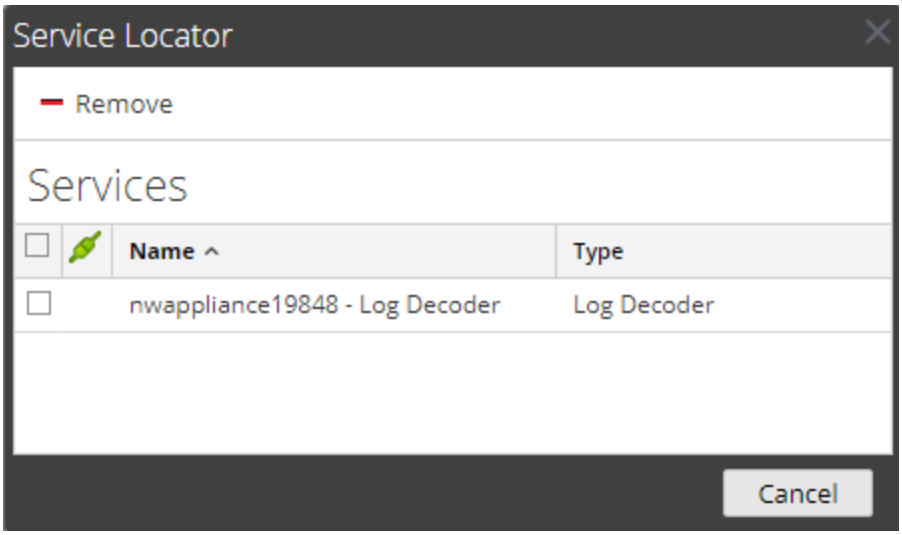
Locate and Remove a Deployed Resource from Services

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.

Remove 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 view > Deployments tab > Subscriptions 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:

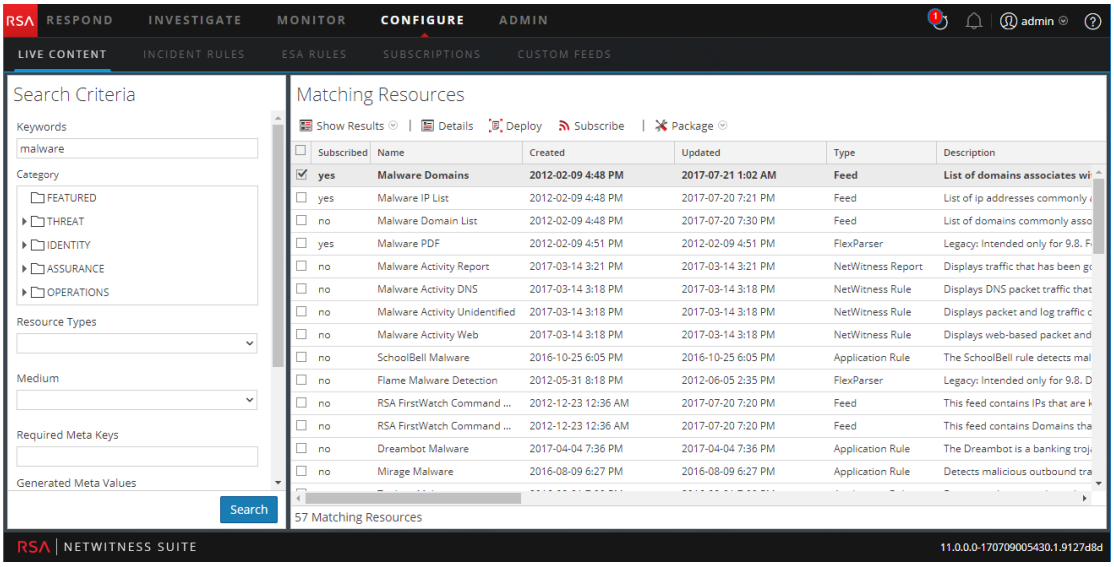
1. In the **Groups** panel, select a group.

   Subscribed resources, if any, are listed in the Subscriptions panel.
2. In the Subscriptions panel, click .

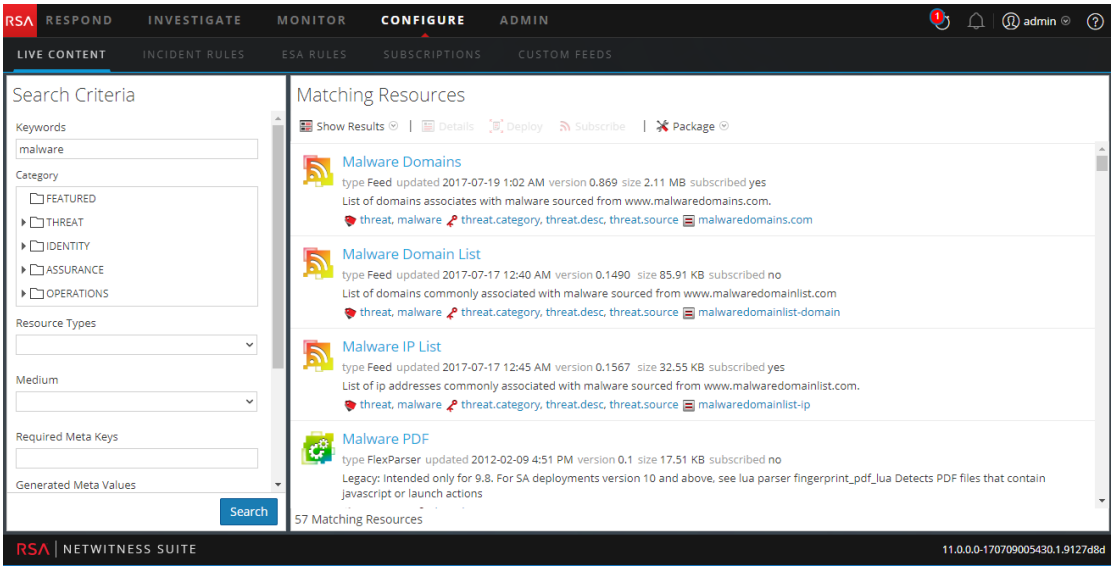
   A dialog requests confirmation that you want to delete the resource from the service group. The resource is removed from the Deployments tab Subscriptions panel, but is not removed from services on which it is deployed.

Show Results as a List or in Detail

1. To change to grid results when viewing detailed results, select **Show Results > Grid**.



2. To change to detailed results when viewing grid results, select **Show Results > Detailed**.



Subscribe and Unsubscribe to a Resource

Subscribe

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

To subscribe to a resource:

1. Navigate to the Live > Search view.
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.

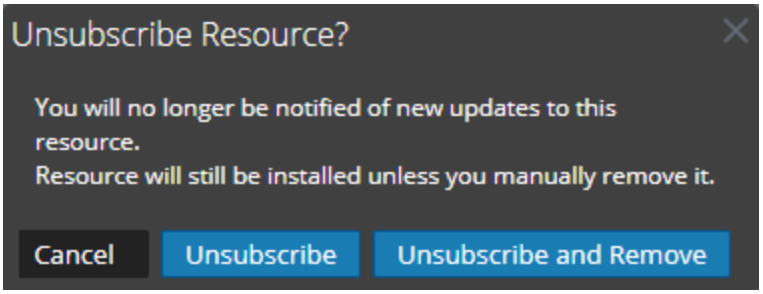
Unsubscribe

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. With a resource displayed in **SUBSCRIPTIONS**, click Unsubscribe.

   A confirmation dialog is displayed.



2. 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.

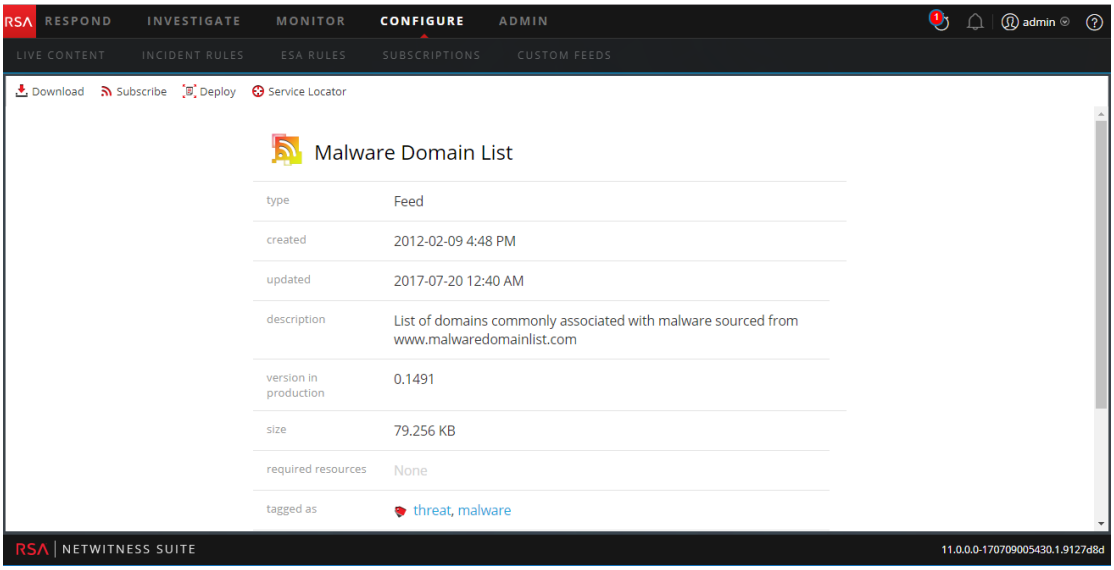
View Resource Details

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.



View Subscribed Resources Selected to Deploy on Services

In the Live Configure view > 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.

Troubleshooting

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

Troubleshooting OutOfMemoryError on Contexthub Server

This section provide troubleshooting instructions when you encounter 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:

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. Decrease the number of parallel threads available for processing STIX, perform the following:
   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.

References

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

- Deployments Tab
- Discontinued Resources Tab
- Live Configure View
- Live Feeds View
- Live Resource View
- Live Search View
- NetWitness Suite Feedback and Data Sharing
- Resource Package Deployment Wizard
- RSA Live Registration Portal
- Subscriptions Tab

Live Configure View

In the Live Configure view, NetWitness Suite 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 Suite Live, please read Live Services Management.

To access this view, go to **CONFIGURE > Subscriptions**. This view has the following tabs:

- Deployments Tab
- Subscriptions Tab
- 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 Suite synchronizes with RSA NetWitness Suite Live. The synchronization schedule is configured in the Live Configuration panel. If you do not want to wait for the scheduled synchronization, you can also tell NetWitness Suite to synchronize now in the Live Configuration panel.

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.

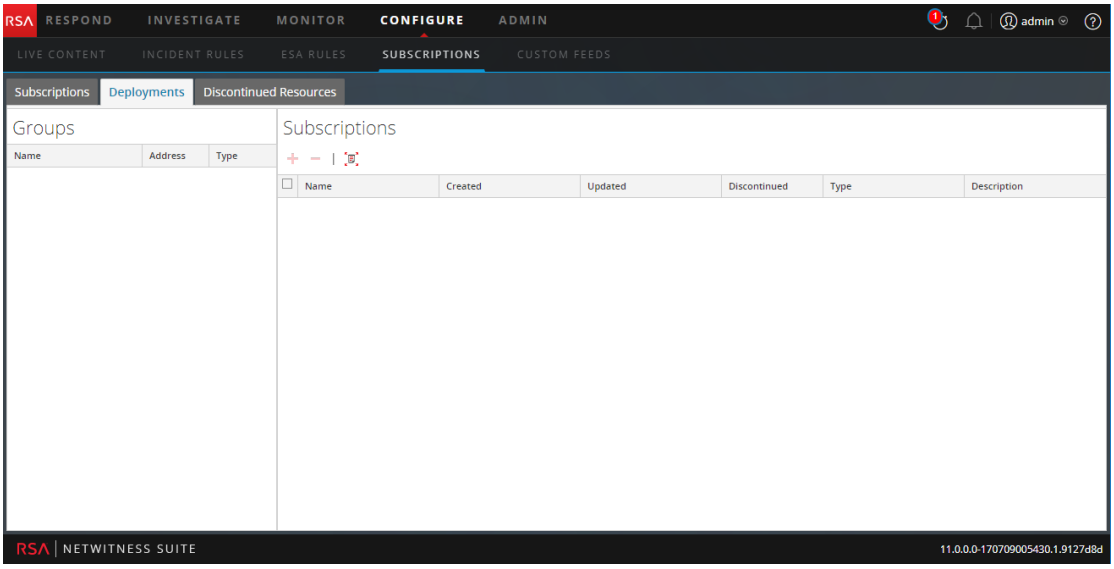
The required permission to access this view is **Manage Live Resources**.

To access this view:

1. Go to **CONFIGURE > Subscriptions**.

   The **Subscriptions** tab is open by default.

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
Name	This is the service group name. Clicking the plus sign displays a nested list of services in the group.
Address	This is the IP address of each service in the group.
Type	This is 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.
Name	This is the name of the resource.
Created	This is the date and time that the resource was created.
Updated	This is the date and time that the resource was last updated.
Type	This is the type of resource.
Description	This is a description of the resource.

Subscriptions Tab

Subscriptions are NetWitness Suite 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 Suite Live. The choices made in the Live Configuration panel determine how often synchronization occurs and if you receive email notifications of updates. 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 Suite is subscribed is listed in this tab.

In the Subscriptions tab, you can:

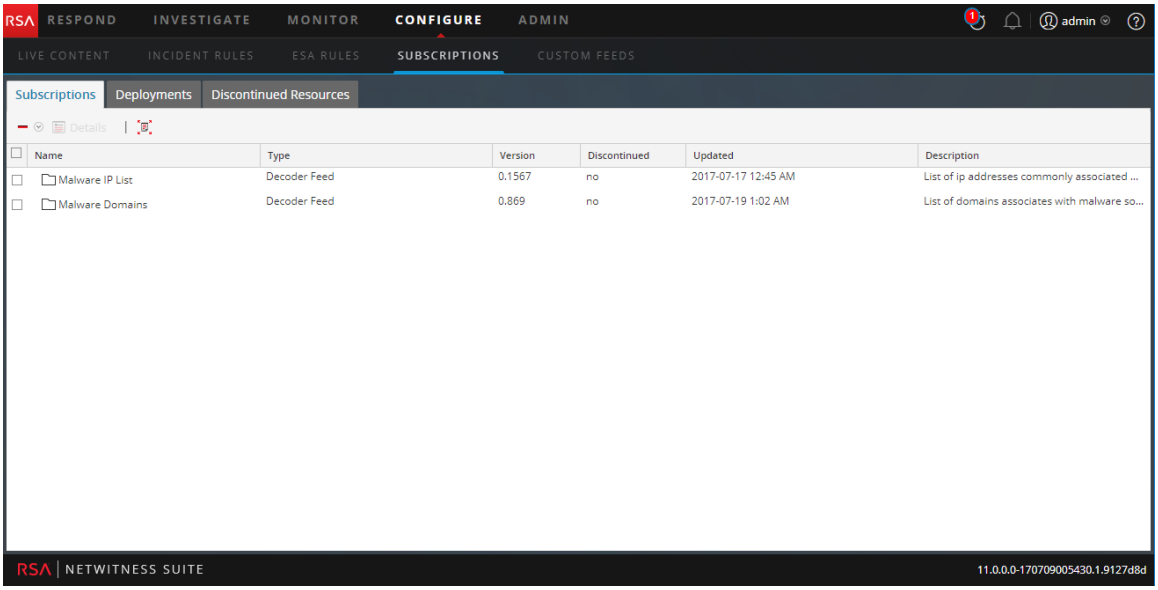
- View all resources to which this NetWitness Suite instance is subscribed.
- Open a detailed view of a subscription in the Live Resource View.
- Delete a subscription.

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**.

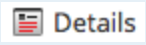
The Subscriptions tab is open by default.



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.
	Displays the details of a single subscribed resource in the Resource View.
	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.
Name	This is the name of the subscribed resource.
Type	This is the type of subscribed resource.
Version	This is the version of the subscribed resource.
Discontinued	Indicates the status of the discontinued resources for the subscribed resource. **Yes** - Resource is discontinued. **No** - Resource is not discontinued. **--** - The Live Server is not checked for the discontinued resources.
Updated	This is the date and time when the subscribed resource was last updated.
Description	This is a description of the subscribed resource.

Discontinued Resources Tab

This topic introduces the features of the **Live Configure view > Discontinued Resources** tab.

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

- Scanning the services for the discontinued resources.
- Removing 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 RSA Link, 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**.

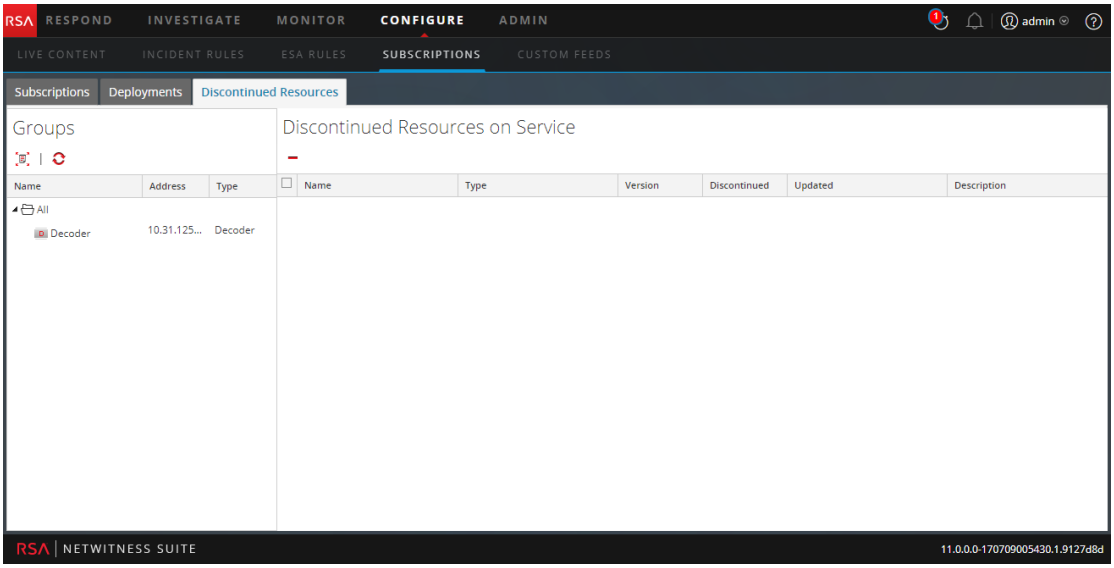
To access this view:

1. Go to t **CONFIGURE > Subscriptions**.

   The **Subscriptions** tab is open by default.

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

   This is an example of the Discontinued Resources tab.



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 deployment on the selected service or service group.

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

Discontinued Resources on Service Panel

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

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

Live Feeds View

Use the Live Feeds View to:

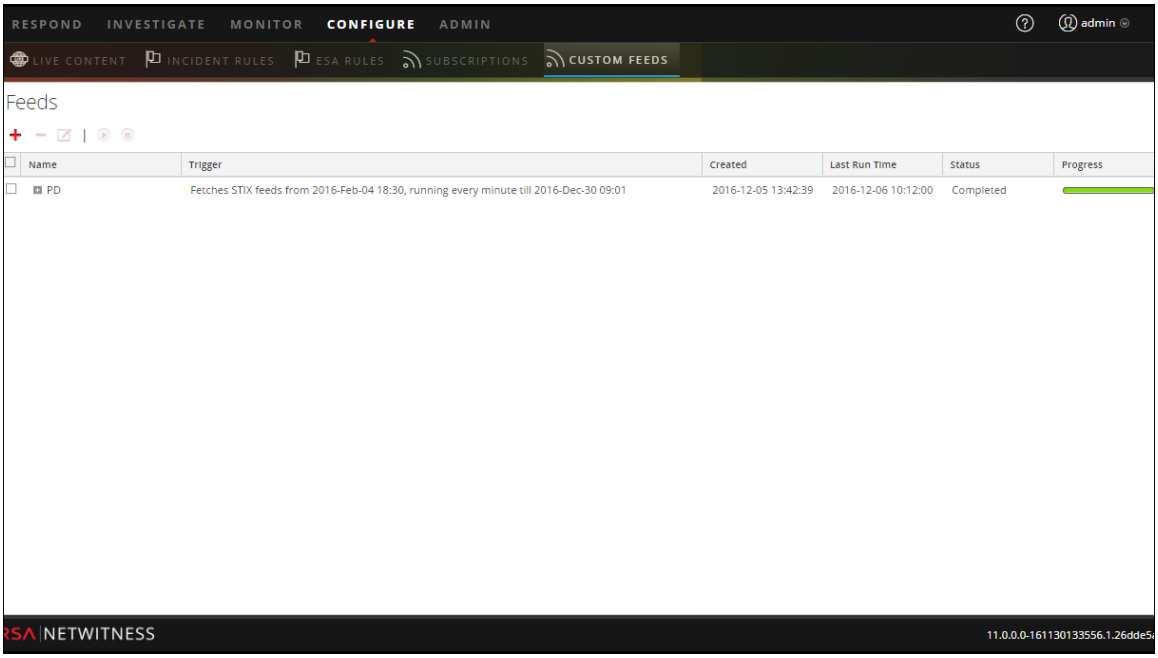
- Create custom feeds.
- Create identity feeds.
- Edit feeds.

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

To access this view, do one of the following:

- In the main menu, select **Live > Feeds.**
- From any view in the Live Module, select **Feeds** in the main menu.

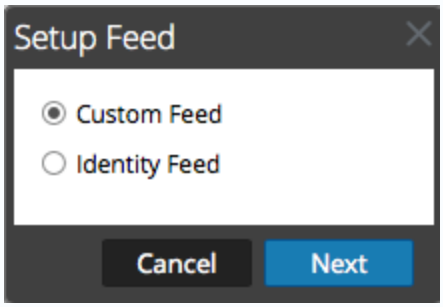
This is an example of the Feeds view.



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

Toolbar

This table describes the options in the toolbar.

Feature	Description
	Initiates the creation of a custom or identify feed by displaying the **Setup Feed** dialog is displayed.  • Custom Feed opens the **Configure a Custom Feed** wizard. • Identity Feed opens the **Configure Identity Feeds** wizard.
	Deletes the feed that you selected.
	Opens the Configure Custom Feed or Configure Identity Feed wizard for the feed that you selected (see Edit a Feed.
	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.
Name	Name of the feed. **Note:** You can now use special characters to define the name of the custom feed.
Trigger	Displays how often the feed runs which is determined by what you defined in **Feed Task Type** when the feed was created.
Created	This is the date and time when the feed was created.

Column	Description
Disk Usage	Displays the MongoDB storage size used by the TAXII feed.
Last Run Time	This is the date and time when the feed was last run.
Status	The status of the feed.
Progress	Progress bar.

Live Resource View

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

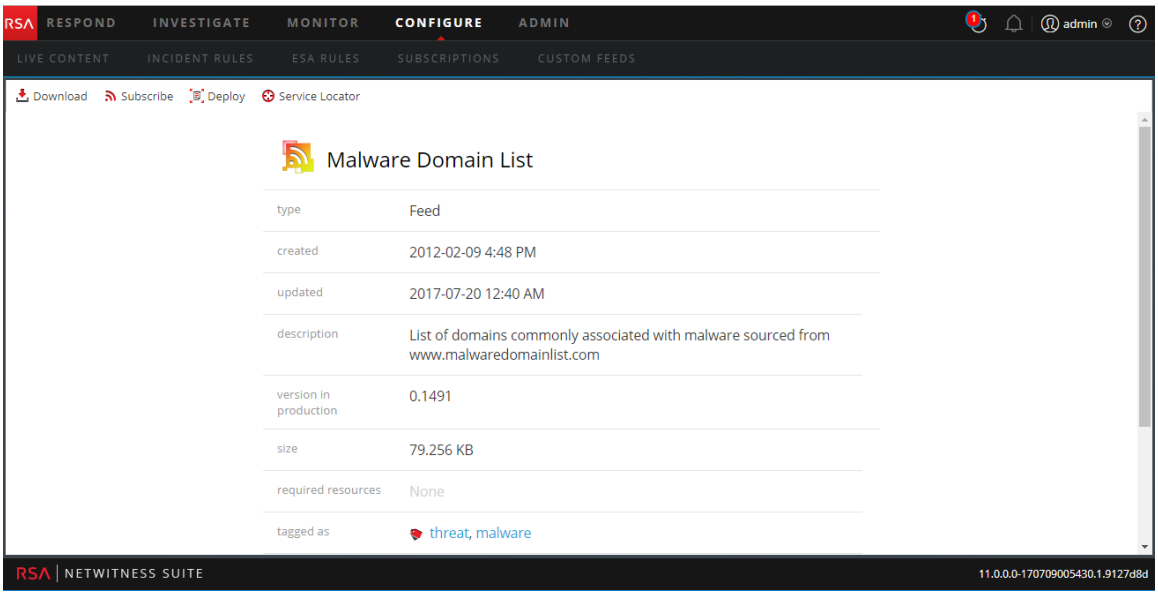
- Download the resource.
- Subscribe or unsubscribe the resource.
- Deploy the resource to services.
- Locate services on which the resource is deployed and remove the resource from services.

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

To access this view, do one of the following:

1. In the main menu, select **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**.

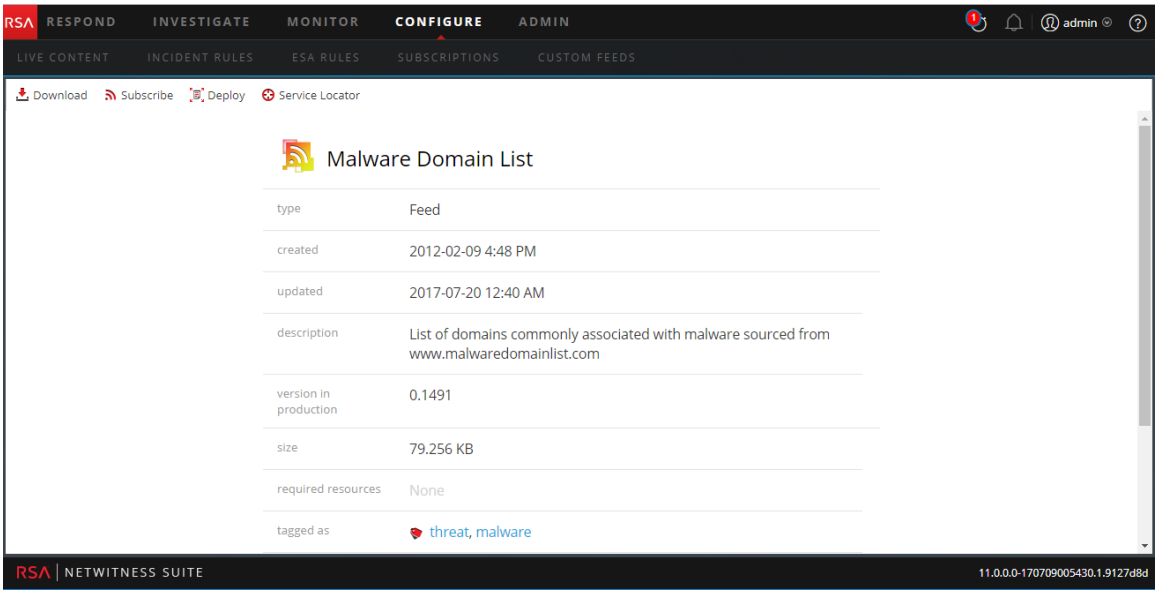
This is an example of the Resource view.



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

Resource Details

This is an example of the resource details displayed in the Resource View.



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

Feature	Description
Resource Type Icon	A graphic representation of the resource type, for example  .

Feature	Description
Name	The name of the resource, for example, **fingerprint_office_lua**.
Type	The type of resource, for example, **RSA Lua Parser**.
Created	The date the resource was created, for example, **2013-09-15 02:16 PM**.
Updated	The date the resource was last updated, for example, **2013-09-15 02:16 PM**
Description	The description of the resource, for example, **Identifies Microsoft Office 95, 2007 Word, Excel, and PowerPoint documents**.
Version in production	The version of the resource, for example, **0.1**.
Size	The size of the resource, for example, **9.079 KB**.
Required Resources	A list of resources on which this resource depends, for example, **NetWitness Lua Library**. Clicking a resource replaces the currently displayed details with the details of the one you clicked.
Tagged as	The tags  that apply to the resource. In the example, the tag is **featured, informational**. Clicking a tag opens the Live Search View with the search narrowed to match resources with that tag.
Required Meta Keys	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.
Generates Meta Values	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.
Permissions	The permissions required for the resource.

Resource View Toolbar

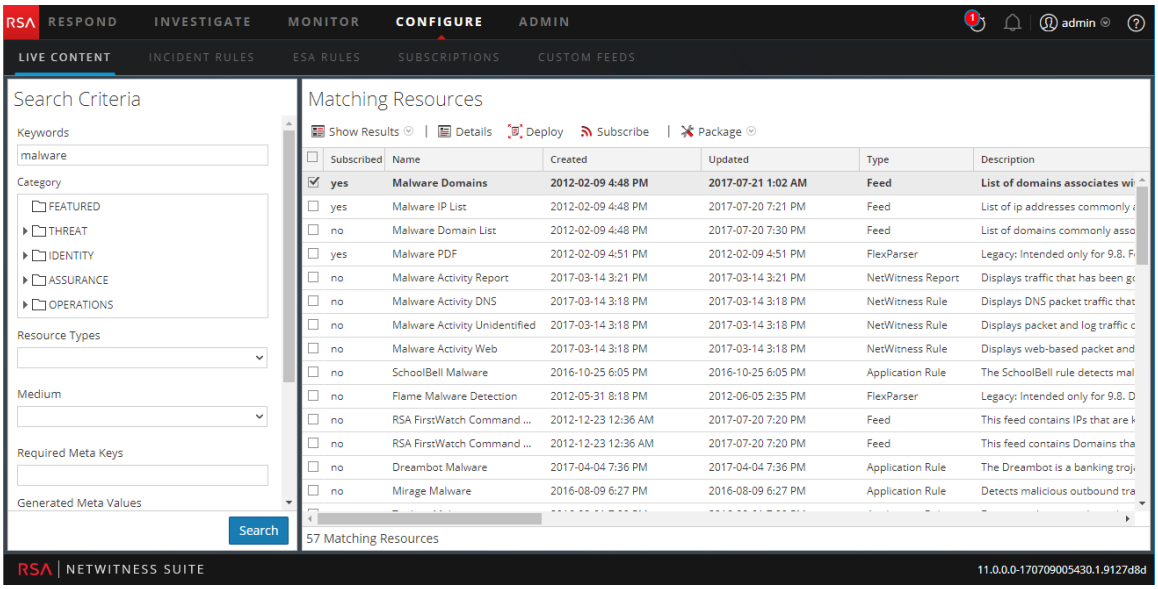
This table describes the Live Resource view toolbar options.

Feature	Icon	Description
Download		This option downloads the resource currently displayed in the Resource View.
Subscribe or Unsubscribe		This option subscribes to or unsubscribes from the resource currently displayed in the Resource View. • Clicking **Subscribe** opens a dialog notifying that you are agreeing to receive notification when the selected resources are updated. You can cancel or click **OK**. • Clicking **Unsubscribe** 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 **Unsubscribe** or **Unsubscribe and Remove**, which also removes the resource from services on which it is deployed.
Deploy		This option provides a way to deploy the resource currently displayed in the Resource View. Clicking **Deploy** opens the Manual Resource Deployment dialog.
Service Locator		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.

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.

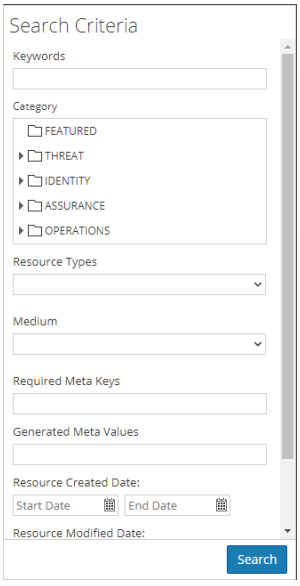
This is an example of the Search view.



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
Keyword(s)	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.
Category	The categories mirror the hierarchical Investigation Model that RSA uses to organize resources. The purpose of the Investigation model is to deliver an accurate path to information security incident response. For more details, see the Investigation Model topic.
Resource Types	Select resources types from the drop-down list to filter resources by type of resource. Possible values are: • Advanced Analytics (Warehouse) • Application Rule • Bundle • Correlation Rule • Event Stream Analysis Rule • Feed • FlexParser • Log Collector • Log Device • Lua Parser • Malware Rules • NetWitness List • NetWitness Report • NetWitness Rule

Feature	Description
Medium	Select one or more mediums from the drop-down list to search for content based on the meta data source. Available values for medium are as follows: • **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
Tags	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 **netwitness for logs** tag. Alternatively, you can click a tag in the Matching Resources panel to insert that tag in this field.
Required Meta Key(s)	Enter a specific meta key; for example, **threat.source**. Alternatively, you can click a meta key in the Matching Resources panel to insert that tag in this field.
Generated Meta Value(s)	Enter a generated meta value; for example, **netwitness**. Alternatively, you can click a generated meta key in the Matching Resources panel to insert that tag in this field.
Research Created Date	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.
Research Modified Date	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.

Feature	Description
Search	Click **Search** to send the search request to the Live server. More specific search criteria return matching resources more quickly.
Cancel	Click **Cancel** to cancel the search in progress.
Include Discontinued Resources	Check **Include Discontinued Resources** to include the discontinued resources in the search result. For an up-to-date list of resources that have been discontinued, see the Discontinued Content topic.

Matching Resources Panel

The Matching Resources panel presents 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
Resource Type Icon	A graphic representation of the resource type. For example  .
Name	The name of the resource, for example, **Group Management**. **Note:** (Discontinued) is displayed next to the resource name if a resource is discontinued.
Type	The type of the resource, for example, **Rule**.
Updated	The date the resource was last updated, for example, **2015-09-15 4:27 PM**.
Version	The version of the resource, for example, **0.1**.
Size	The size of the resource, for example, **153 B**.

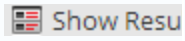
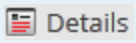
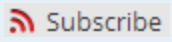
Feature	Description
Subscribed	Subscription status: • **yes**: This NetWitness Suite instance is subscribed to this content resource. • **no**: This NetWitness Suite instance has not subscribed to this content resource.
Description	The description of the resource, for example, **Compliance Rule-Group Management**.
Tags	The tags that apply to the resource. Clicking a tag narrows the search to resources with that tag. For example,  .
Meta Keys	The meta keys that apply to the resource. Clicking a meta key narrows the search to resources with that meta key. For example,  .
Resource Meta Values	The meta values generated by the resource. Clicking a meta value narrows the search to resources that generated the meta value. For example,  .

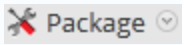
Grid Results

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

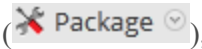
The following table describes the elements in the grid results.

Feature	Description
Subscribed	Subscription status: • **yes**: This NetWitness Suite instance is subscribed to this content resource. • **no**: This NetWitness Suite instance has not subscribed to this content resource.
Name	The name of the resource, for example, **Group Management**. **Note:** The resource name is displayed in red color if it is discontinued.
Created	The date the resource was created, for example, **2015-08-12 3:11 PM**.

Feature	Description
Updated	The date the resource was last updated, for example, **2015-09-15 4:27 PM**.
Type	The type of the resource, for example, **Rule**.
Discontinued	The status of the discontinued resources: **yes** - The resource that matches the search criteria is discontinued. **no** - The resource is not discontinued. **--** - The Live Server is not checked for the discontinued resources.
Description	The description of the resource, for example, **Compliance Rule-Group Management**.
Toolbar	
	This menu offers two ways to view search results: **Detailed** and **Grid**.
	This option applies to a single selected resource. Clicking **Details** opens the selected resource in the Live Resource view.
	This option applies to one or more selected resources.
	This option applies to one or more selected resources. Clicking **Subscribe** opens a dialog that asks for confirmation that you want to receive notification when the selected resources are updated.

	This menu offers two packaging functions for the selected resources:
	• **Create**: creates a **resourceBundle.zip** file that contains the selected resources and opens a dialog in which you can either:
	  • open the file, or
	  • save the file for subsequent deployment.
	• **Deploy**: opens the Deployment Wizard, in which you can choose a **resourceBundle.zip** file and deploy it.

See Also

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

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 Suite accepts packages in **.nwp** files or **.zip** files.

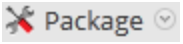
Deploying resources manually deploys them directly to the services without taking advantage of the powerful resource management capabilities of NetWitness Suite.

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.

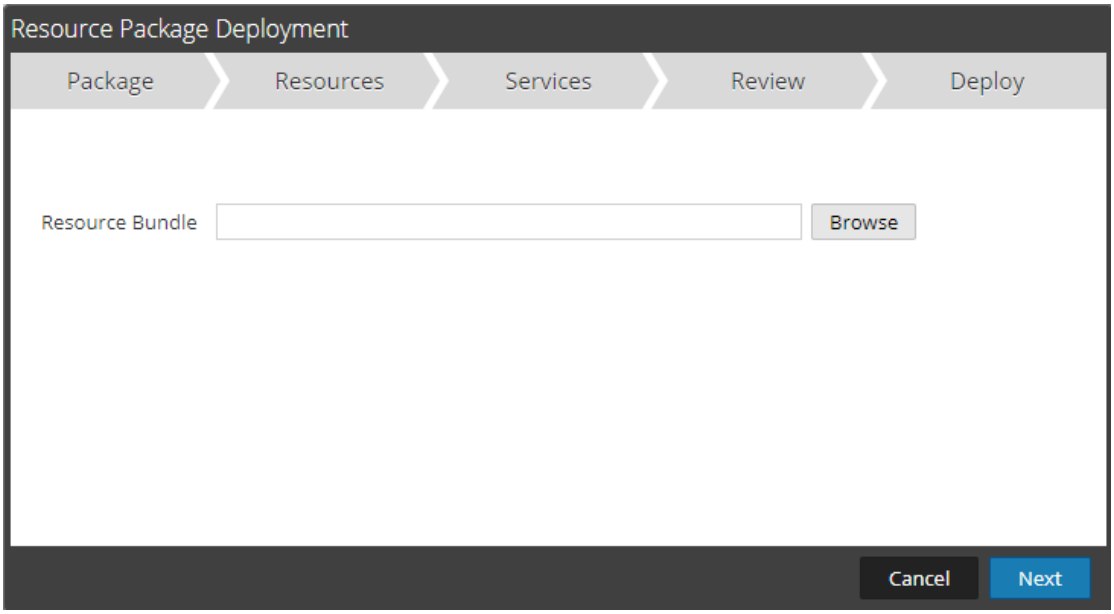
Note: Use NetWitness Suite Live to create resource bundles; this is a different application that is not part of NetWitness Suite. Selecting **Package** > **Create** in the **Live Search - Matching Resources** toolbar displays the Content Package Tool window. You can choose resources to include in a package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

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

To access this view:

1. In the main menu, select **CONFIGURE > Live Content**.
2. In the **Live Search - Matching Resources** toolbar, select  > **Deploy**.

The Resource Package Deployment wizard is displayed.



Features

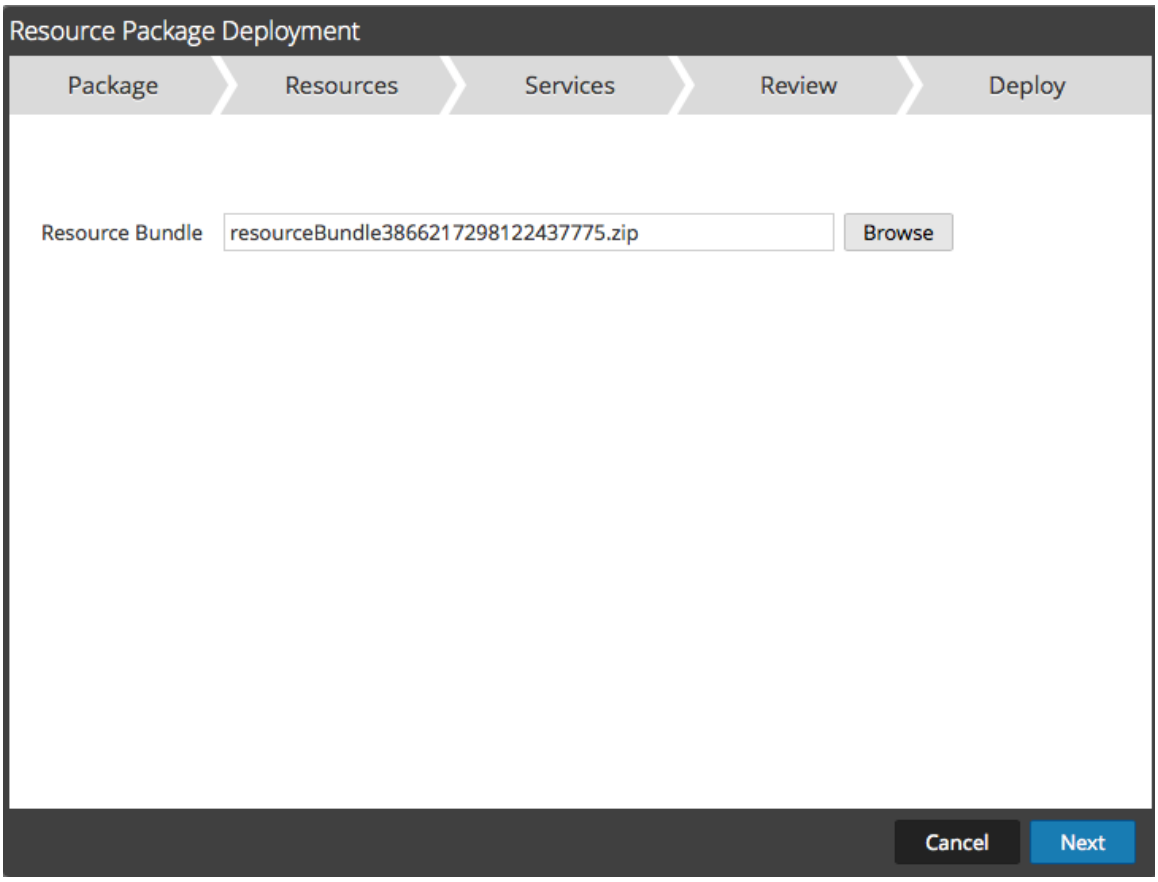
The Deployment Wizard has five tabs: **Package, Resources**, **Services**, **Review** and **Deploy**. Use **Close** to exit before you complete the wizard.

When you complete the wizard, NetWitness Suite 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.



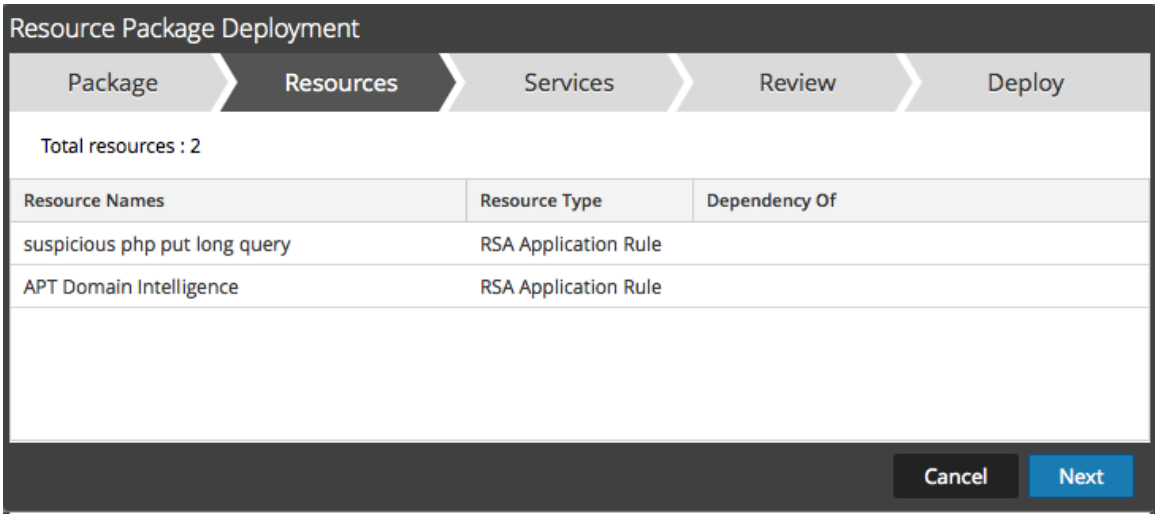
The following table describes the elements in the Package tab.

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

Resources Tab

This tab displays the resources contained in the bundle.

The following figure shows an example of the Resources tab.



The following table describes elements in the Resources tab.

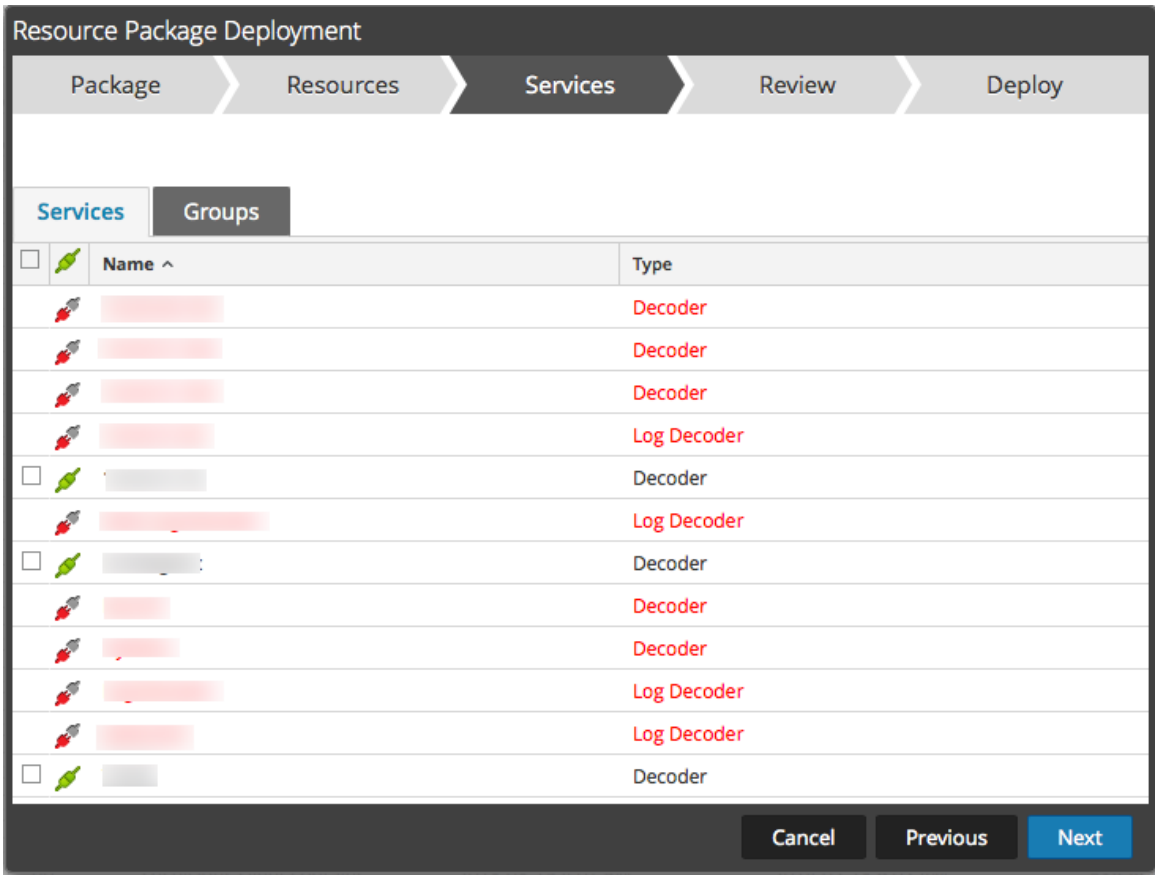
Column	Description
Resource Name	Displays the name of the resources in the bundle (for example, **NetWitness Lua Library**).
Resource Type	Displays the resource types for the resources in the bundle (for example, **RSA Lua Parser**)
Dependency Of	Displays Resources on which the selected resource depends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

Services Tab

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

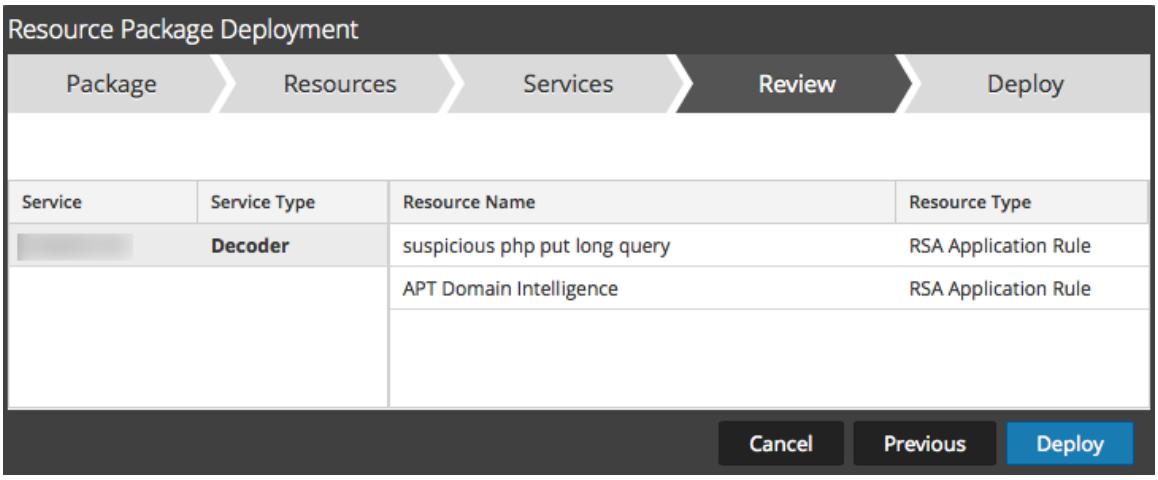
Review Tab

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.

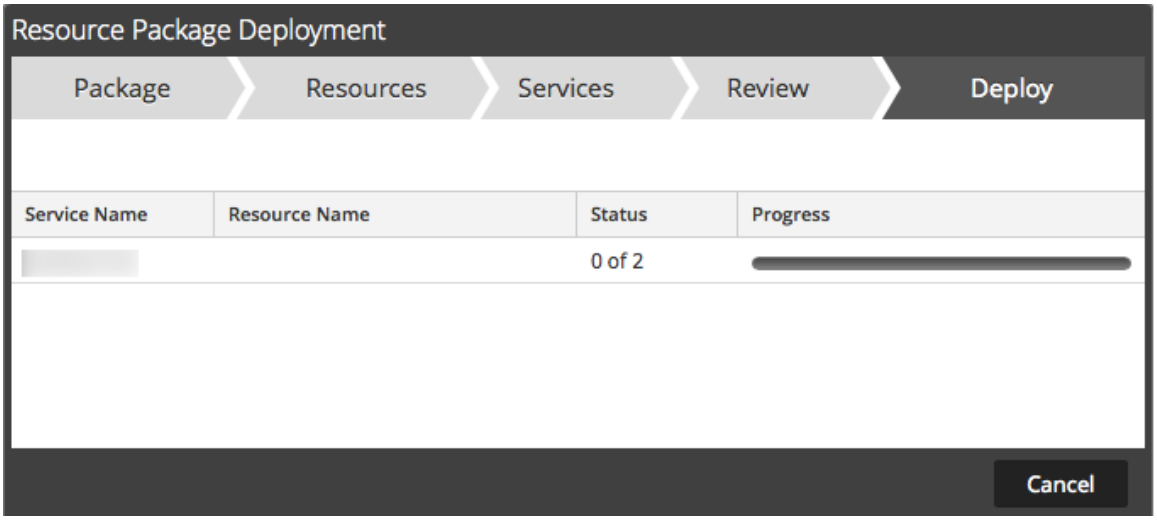
Column	Description
Service Information	
Service	Displays the services in your environment to which you can deploy the content.
Service Type	Displays the type of each NetWitness Suite service (type of host/service).
Resource Information	
Resource Name	Displays the name of the resources you have selected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



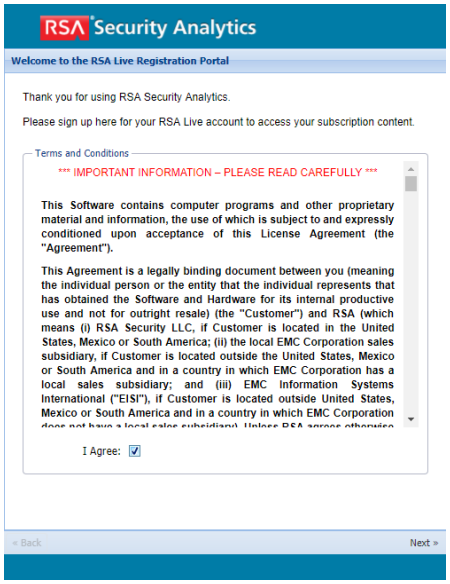
The following table describes the elements in the Deploy tab.

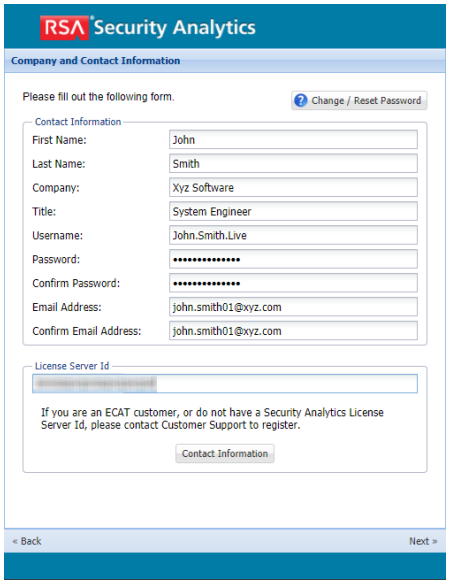
Feature	Description
Service Name	Name of the services to which resources are deployed.
Resource Name	Name of the resources.
Status	Status of the manual deployment.
Progress	Progress of the manual deployment in a progress bar. When complete, the bar is solid green.
Command Buttons	
Close	Closes the wizard.

Feature	Description
Errors	Only displays if NetWitness Suite encountered any errors. Click to display the errors.
Retry	Only displays if NetWitness Suite encountered any errors. Click this button to try to deploy the resources again using the wizard.

RSA Live Registration Portal

The RSA 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 RSA Live library. To access the portal, go to the following URL: https://cms.netwitness.com/registration/.





After you agree to the Terms and Conditions, click **Next**: the fields for setting up an account are displayed. These include Contact Information, Subscription Level, and License Server Id.

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

Parameter	Description
Change / Reset Password	Allows users to change or reset their RSA Live password.
First Name	Your first name.

Parameter	Description
Last Name	Your last name.
Company	The name of your company.
Title	Your job title or function in the company.
Username	The username used to log on to RSA Live account. The username must contain a minimum of nine characters and a maximum of 60 characters.
Password	The password for the RSA Live account. The password must contain minimum of nine characters and the maximum length is 60, with at least one uppercase, one lowercase, one number, and one special character.
Confirm Password	Confirmation of your password.
Email Address	The email address where you want to receive notifications related to the Live account.
Confirm Email Address	Confirmation of the email address.
Subscription Level / Confirm Subscription Level	• **Basic** - This provides access to the Live content that is tagged for groups like Basic, Panorama for Log Decoder, and Spectrum for Malware Analysis. • **Enhanced** - This provides access to the Live content that is tagged for groups like Enhanced, Basic, Panorama for Log Decoder, and Spectrum for Malware Analysis. • **Premium** - This provides access to the Live content that is tagged for groups like Premium, Verisign Premium, Enhanced, Basic, Panorama for Log Decoder, and Spectrum for Malware Analysis.
License Server Id	This is the License Id on the **ADMIN > SYSTEM > Info** page. **Caution:** The license server ID on NetWitness Suite must be valid and must be registered on the Flexera Server. If not, contact RSA Customer Support.

NetWitness Suite Feedback and Data Sharing

This topic introduces the Feedback and Data Sharing features of NetWitness Suite.

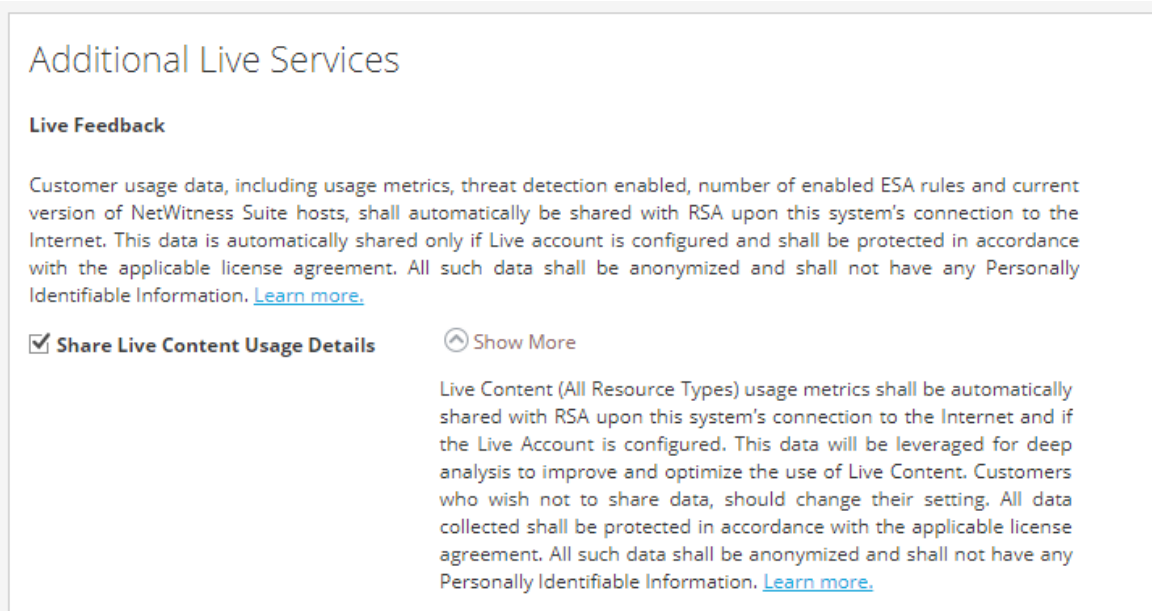
The settings for these features are available in **ADMIN** > **SYSTEM** > **Live Services** view, in the Additional Live Services section.

Additional Live Services

Participation in the Additional Live Services is configured in the **ADMIN > SYSTEM > Live Services** view.

Live Feedback

Live Feedback is intended to help improve RSA NetWitness Suite.



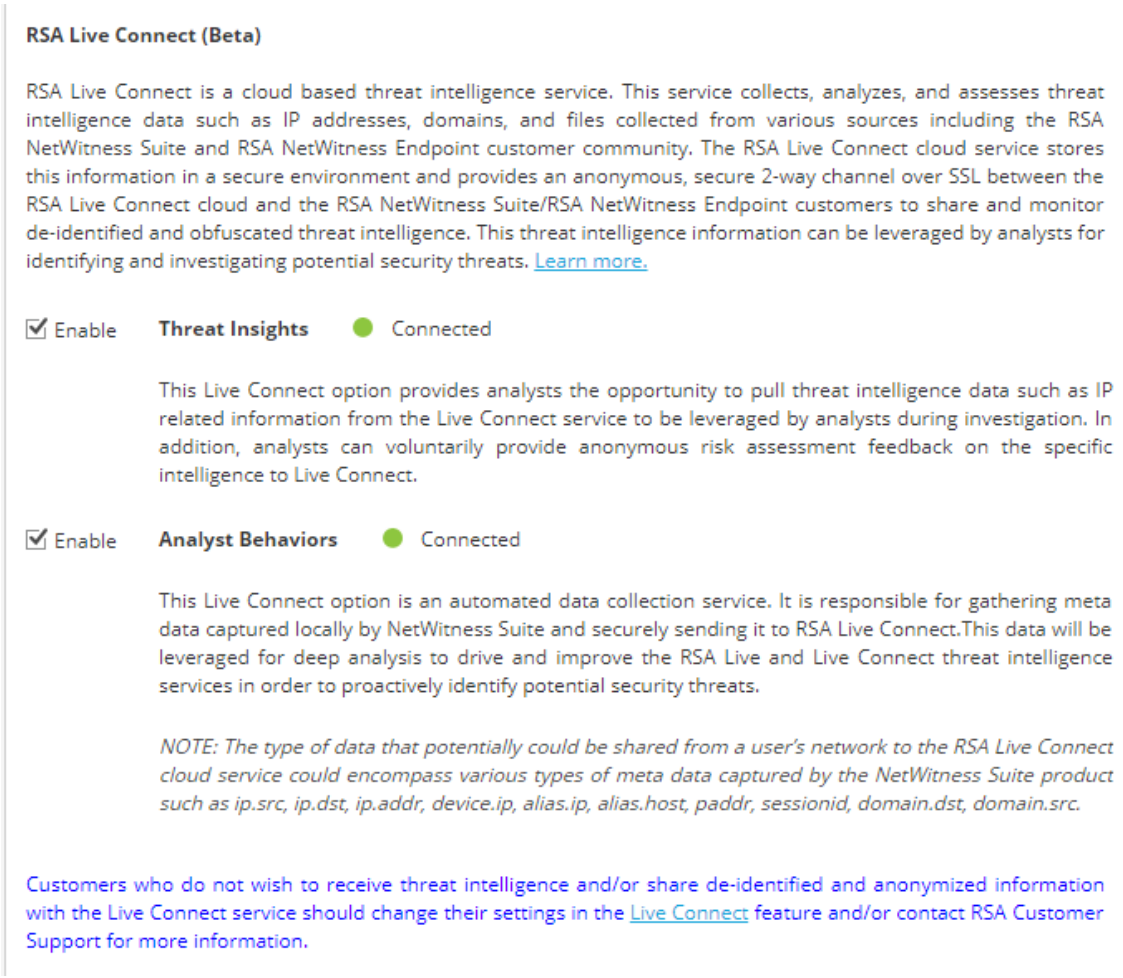
Once you set up and configure a Live account, usage data is shared with RSA. This data is automatically shared only if Live account is configured and shall be protected in accordance with the applicable license agreement. All such data shall be anonymized and shall not have any Personally Identifiable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

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

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

RSA Live Connect

RSA Live Connect is a cloud based threat intelligence service. This service collects, analyzes, and assesses threat intelligence data such as IP addresses, domains, and files collected from various sources including the RSA NetWitness Suite and RSA ECAT customer community.



RSA Live Connect consists of the following features:

- Threat Insights
- Analyst Behaviors

Threat Insights

Threat Insights provides analysts the opportunity to pull threat intelligence data such as IP related information from the Live Connect service to be leveraged by the analysts during investigation.

By default, **Threat Insights** is enabled in **Additional Live Services** section. If Context Hub service is configured, Live Connect is automatically added as a data source for Context Hub. For more information, see the **Configure Live Connect Data Source for Context Hub** topic in the *Context Hub Configuration Guide*.

With Live Connect as a data source for context hub, you can use the Context Lookup option in Investigation > Navigate view or Investigation > Events view to fetch contextual information. For instructions, see View Additional Context for a Data Point.

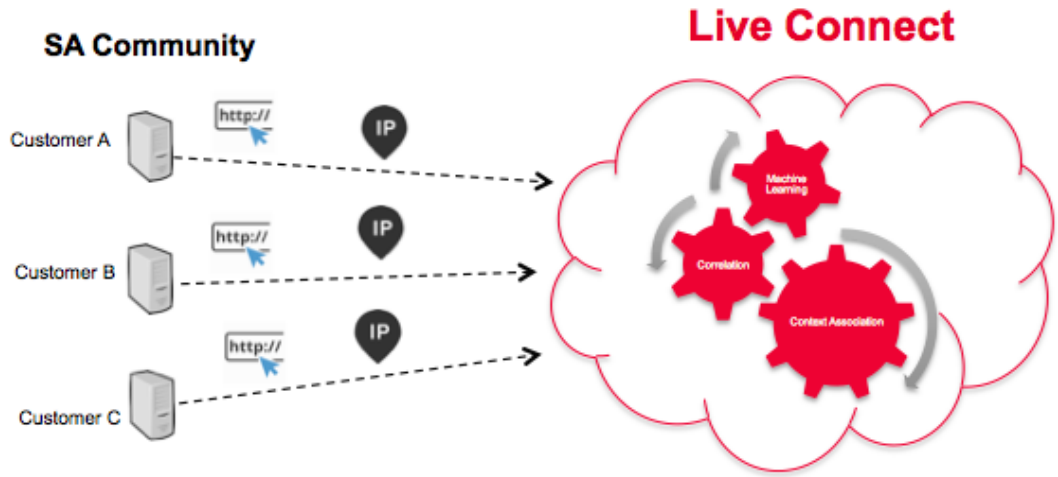
Analyst Behaviors

Analyst Behaviors is a feature where analysts participate in sharing data to RSA community. This is an automated data collection service. Its goal is to share potential threat intelligence data to the RSA Live Connect cloud service for analysis. The type of data that could be shared from your network to RSA Live Connect includes various types of meta data captured by NetWitness Suite such as ip.src, ip.dst, ip.addr, device.ip, alias.ip, alias.host, paddr, sessionid, domain.dst, domain.src.

Note: All data collected locally is de-identified and obfuscated and then sent securely and anonymously to the RSA Live Connect cloud service, where it is stored in a secure environment.

Description

Live Connect Threat Data Sharing has been developed as a Community based threat intelligence sharing platform.



It has the following characteristics and goals:

- Crowd-sourced: the RSA community contributes to the entire collection of intelligence
- Centrally collect and analyze data from the RSA community

- Reduce the intelligence cycle time from days to minutes

Some details to consider:

- We are leveraging analyst investigation activity
- We are harvesting meta data such as IP addresses and domain names
- We are doing deep data analysis: Trending, correlation, anomaly detection
- Remember, this feature is currently in Beta

Participation

Customer participation is optional. Upon initial install or upgrade to NetWitness Suite 11.0, you are presented with a confirmation screen. By default, you are entered into the program, but you can opt out at any time.

Cloud Authentication

Authentication for the program is done in the NetWitness Suite UI, where you configure the Live account in the Live services section.

Configuration

To view or change the settings for Live Connect Threat Data Sharing, in the main menu, select **ADMIN > SYSTEM > Live Services**. Check or clear the **Enable** box to participate or stop participating in the program.

Data Collection

Data is collected as follows:

- Data Attribution: Anonymous
- Data Source: Subset of meta keys and meta values of a NetWitness Suite analyst's page views from the NetWitness Suite Core Query logs.
- Query Log Harvesting Process:
  - Timing: Batch mode every 24 hours (4 AM – 6 AM UTC)
  - Log Collection: NetWitness Suite server collects NetWitness Suite core device log entries for the previous 24 hours
  - Log Entries: Only SDK-Value and SDK-Query API calls that contain a where clause are collected
  - Log Attribute Parsing: Each entry must have one of the following meta key indicators present: **ip.src**, **ip.dst**, **ip.addr**, **device.ip**, **alias.ip**, **alias.host**, **paddr**, **sessionid**,

domain.dst, or **domain.src**. If so, meta keys and meta values from the entry will be collected.

Note: Once the above criteria is met, NetWitness Suite sends all of the meta keys and values from the query to the cloud—not just the meta key indicators.

The log report is sent in JSON format, over SSL. It contains:

- Timestamps
- Live CMS username (sha256)
- NetWitness Suitelicense server ID (sha256)
- List of SA endpoint IDs (sha256)
- Harvested meta values (MD5 and SHA256 hashed)

Example

This section lists entries from a log, and then the corresponding section of extrapolated data.

Section from a log file:

```
User admin (session 204298, 10.4.50.60:57454) has issued values (channel 205237)
(thread 2332): fieldName=filter id1=1 id2=23138902 threshold=100000 size=20
flags=sessions,sort-total,order-descending,ignore-cache where="(alias.host =
'mail.google.com') && (ip.src = 161.253.31.130) && time=\"2015-12-07 18:08:00\"-
\"2015-12-07 21:07:59\""
```

Data extrapolation with hashing:

```
{
    timestamp: 1452282588000,
    session: 204298,
    id1: 1,
    id2: 23138902,
    userName: "8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918",
    loggerName: "SDK-Values",
    timeRange: "\"2015-12-07 18:08:00\"-\"2015-12-07 21:07:59\"",
  - metaList: [
      - {
            metaKey: "alias.host",
          - properties: {
                domain_hint: "mai*********.com",
                domain_tld: "com",
                md5_value: "be5cab0695415d9363d18ad1345c73eb",
                sha256_value: "3f2728499a4b29460f3e3150df508e06b19edf0f58efd051fac777844d28e452"
            }
        },
      - {
            metaKey: "ip.src",
          - properties: {
                md5_value: "03b81ffdff109a05a3dac88dbec10c59",
                sha256_value: "1d88c6893797c896070bd5470d0026e11b515d5dee97c6173771a43719fa7e78"
            }
        }
    ]
},
```


Troubleshooting

This section discusses a bit about troubleshooting Live Connect Threat Data Sharing.

Query Log Retrieval Sample

To retrieve a sample of threat intelligence data sent to Live Connect, you 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 to use 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

You can access some debug information as follows.

1. Select **ADMIN > SYSTEM > System Logging**.
2. Select the **Settings** tab.

3. In the Package Configuration section, select **com > netwitness > platform > server > liveconnect > service (DEBUG)**.