



# Decoder and Log Decoder Configuration Guide

for Version 11.0



## **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](http://www.emc.com/legal/emc-corporation-trademarks.htm#rsa).

## **License Agreement**

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

## **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**

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

October 2017

# Contents

---

<b>Decoder and Log Decoder Quick Setup .....</b>	<b>9</b>
Perform Initial Quick Setup .....	11
<b>Configure Common Settings on a Decoder .....</b>	<b>13</b>
Configure Capture Settings .....	15
Select a Network Adapter .....	15
Configure a Decoder to Begin Capturing Data Automatically .....	17
Configure Optional Capture Settings .....	18
(Optional) Configure System-Level (BPF) Packet Filtering .....	19
(Optional) Configure a Decoder to Capture Data Across All Types of Network Interfaces .....	22
(Optional) Preserve VLAN Tags When Using the Packet MMAP Capture Interface .....	25
Enable and Disable Parsers and Log Parsers .....	29
Start and Stop Data Capture .....	32
<b>Configure Decoder Rules .....</b>	<b>33</b>
Rule Processing .....	34
Rule Configuration .....	34
Rule and Query Guidelines .....	34
Rule Examples .....	35
Invalid Rules .....	35
General Syntax Guidelines .....	36
Capture Rule Syntax .....	36
Configure Capture Rules .....	40
Import Rules from a File and Export Rules .....	42
Push Rules to Other Services .....	44
Change Execution Order of Rules .....	46
Restore a Rule Snapshot from History .....	46
Configure Application Rules .....	48
Configure Correlation Rules .....	52
Configure Network Rules .....	56
Supported Meta Keys in Network Rule Conditions .....	56
Fix Rules with Invalid Syntax .....	61
Decoder Commands for Managing Rules .....	63

add Command .....	63
merge Command .....	64
Methods of Sending a List of Rules to a Service .....	65
Ordering Rules When Pushing .....	66
replace Command .....	67
clear Command .....	68
delete Command .....	68
validate Command .....	68
<b>Configure Feeds and Parsers .....</b>	<b>69</b>
Configure Parsers .....	69
Configure Feeds .....	70
Custom Feed Definition File Structure .....	71
Sample Feed Definition File .....	71
Feed Definition Equivalents for Custom Feed Wizard Parameters .....	72
Sample Files for a MetaCallback Feed Using CIDR Index Range for IPv4 and IPv6 .....	75
Create a Custom Feed .....	77
Create a STIX Custom Feed .....	89
Create an Identity Feed .....	100
Import the SSL Certificate .....	109
Cannot Verify Identity Feed URL .....	110
Edit, Upload, or Remove a Feed .....	112
Create Custom Meta Keys Using a Custom Feed .....	117
Add a Custom Meta Key in the Log Decoder .....	117
Deploy a Log Decoder Feed in Live .....	117
Add the Custom Meta Key Entry in the Concentrator Custom Index file .....	123
Investigate on the Custom Meta Key .....	124
Additional Procedures .....	125
Upload and Delete Custom Parsers .....	129
Upload Parsers to a Decoder or Log Decoder .....	129
Manage Upload Jobs .....	131
Delete Deployed Parsers .....	131
Enable and Configure the Entropy Parser .....	132
Entropy Parser Configuration in the Concentrator Custom Index File .....	135
<b>Decoder and Log Decoder Additional Procedures .....</b>	<b>138</b>
Configure 10G Capability .....	139

Hardware Prerequisites .....	139
Software Prerequisites .....	140
Install the 10G Decoder .....	140
Configure the 10G Decoder .....	141
Storage Considerations .....	143
Parsing and Content Considerations .....	143
Configure a Log Decoder to Accept Protobuf .....	147
Configure Session Split Timeouts .....	149
Configure Syslog Forwarding to Destination .....	152
Configure Transaction Handling on a Decoder .....	155
Transaction Handling .....	155
Decrypt Incoming Packets .....	157
Performance Considerations .....	158
Encryption Keys .....	160
Upload Multiple Premaster and Private Keys .....	162
Parameters for Managing Keys .....	164
Return Values .....	164
Viewing Unencrypted Traffic .....	165
Edit Decoder System Configuration .....	166
Enable CPU Usage Statistics for Installed Content .....	168
Enable Parser Mappings .....	169
Enable IP Address to Event Source Mapping .....	169
Update IP to Event Source Mapping .....	170
Read IP to Event Source Type Mappings .....	171
Edit an IP to Event Source Type Mapping .....	172
Delete an IP to Event Source Type Mapping .....	172
Sort the Hostname or Event Source Type .....	172
Import IP to Event Source Mapping Entries .....	173
Export IP to Event Source Mapping Entries .....	174
Search IP to Event Source Mapping Entries .....	174
Enable or Disable Lua and Flex Parsing Systems .....	175
Map IP Address to Service Type for Log Parsing .....	176
Map an IP Address to a Service Type .....	176
Map an IP Address to a Time Zone .....	177
Obtain Log Files a from Pre-11.0 Log Decoder .....	178
Upload a Log File to a Log Decoder .....	181

Upload a Packet Capture File .....	183
<b>Feed and Parser References .....</b>	<b>185</b>
Feed Definitions File .....	186
feed-definitions.xml .....	186
Flex Parsers .....	187
NwFlex.xml .....	187
Arithmetic Functions .....	189
Common Parser Operations .....	191
General Functions .....	194
Logging Functions .....	197
Nodes .....	198
Payload Functions .....	205
Regex .....	208
String Functions .....	209
Geo IP Parser .....	213
GeoPrivate.ipl .....	213
Lua Parsers .....	214
List of Lua Parsers .....	214
Search Parser .....	215
search.ini .....	215
search.ini Search String Syntax .....	216
Wireless LAN Configuration .....	218
wlan-config.xml .....	218
<b>Decoder and Log Decoder References .....</b>	<b>220</b>
Services Config View - Data Privacy Tab .....	221
What do you want to do? .....	221
Related Topics .....	221
Quick Look .....	222
Services Config View - Data Retention Scheduler .....	223
What do you want to do? .....	223
Related Topics .....	223
Quick Look .....	223
Services Config View - Feeds Tab .....	225
What do you want to do? .....	225
Related Topics .....	225

Quick Look .....	225
Upload Feeds Dialog .....	227
What do you want to do? .....	227
Related Topics .....	227
Quick Look .....	227
Services Config View - Files Tab .....	230
What do you want to do? .....	230
Related Topics .....	230
Quick Look .....	230
Services Config View - General Tab .....	232
Workflow .....	232
What do you want to do? .....	232
Related Topics .....	232
Quick Look .....	232
Services Config View - Parsers Tab .....	241
What do you want to do? .....	241
Related Topics .....	242
Quick Look .....	242
Services Config View - Parser Mappings Tab .....	244
What do you want to do? .....	244
Related Topics .....	244
Quick Look .....	244
Services Config View - Rules Tabs .....	247
Workflow .....	247
What do you want to do? .....	247
Related Topics .....	248
Quick Look .....	248
App Rules Tab .....	251
What do you want to do? .....	251
Related Topics .....	251
Quick Look .....	251
Correlation Rules Tab .....	255
What do you want to do? .....	255
Related Topics .....	255
Quick Look .....	255
Network Rules Tab .....	258

What do you want to do? .....258

Related Topics .....258

Quick Look .....258

Services System View - Decoders .....263

Workflow .....263

What do you want to do? .....263

Related Topics .....264

Quick Look .....264



## Decoder and Log Decoder Quick Setup

---

A basic RSA Network Suite network includes at minimum Brokers, Concentrators, and Decoders. Brokers aggregate data from Concentrators, and Concentrators consume data from at least one Packet Decoder or Log Decoder. The basic network may include both types of Decoders. Packet Decoders are usually referred to as Decoders, and they capture network data in packet form. Log Decoders capture log data as events.

**Adding a Decoder** makes it visible and available for use with NetWitness SuiteAdministration, Live Services, and Investigate. To add a service in NetWitness Suite, you select the service type, provide service connection information, and validate that the service can be reached. The *Hosts and Services Getting Started Guide* provides the information you need to understand and install all NetWitness Suite services.

After the services are added, you need to configure each service. This is the preferred order for configuring your system:

1. Decoders
2. Log Decoders
3. Concentrators (refer to the *Broker and Concentrator Configuration Guide*)
4. Brokers (refer to the *Broker and Concentrator Configuration Guide*)

**Note:** A Log Decoder is a special type of Decoder, which is configured and managed in a similar way to a Decoder. Most of the information in this guide refers to both types of Decoders. "Decoder" refers to both types of Decoders. Information that applies exclusively to Packet Decoders or Log Decoders is clearly identified.

**Basic Configuration of the Decoder** involves selecting a network adapter interface and starting data capture.

In addition, you can configure each Decoder to control the type of traffic captured using rules, feeds, and parsers. Advanced configuration tasks enable additional features that are relevant to specific applications. For example, configure a 10G Decoder, create custom meta keys, or decrypt incoming packets.

The easiest way to configure all of the required Decoder and Log Decoder settings is to use the options in the NetWitness Suite user interface. For the most part, configuration is performed in the Administration Services view (ADMIN > Services).

The screenshot shows the 'SERVICES' tab in the NetWitness Suite interface. On the left, there is a 'Groups' sidebar with a tree view showing 'All' (25 items). The main area displays a table of services. The 'Decoder' service is selected, indicated by a checkmark in the 'Name' column and a highlighted row.

Name	Licensed	Host	Type	Version	Actions
Broker	✓	NWAPPLIANCE8017	Broker	11.0.0.0-0	[Gear] [Down Arrow]
Broker	✓	NWAPPLIANCE5425	Broker	11.0.0.0-0	[Gear] [Down Arrow]
Concentrator	✓	NWAPPLIANCE19263	Concentrator	11.0.0.0-0	[Gear] [Down Arrow]
Config Server	✓	NWAPPLIANCE8017	Config Server	11.0.0.0	[Gear] [Down Arrow]
Contexthub Server	✓	NWAPPLIANCE17000	Contexthub Server	11.0.0.0	[Gear] [Down Arrow]
<b>Decoder</b>	✓	<b>NWAPPLIANCE1403</b>	<b>Decoder</b>	<b>11.0.0.0-0</b>	[Gear] [Down Arrow]
Event Stream Analysis	✓	NWAPPLIANCE17000	Event Stream Analysis	11.0.0.0.376-1	[Gear] [Down Arrow]
Event Stream Analytics Server	✓	NWAPPLIANCE17000	Entity Behavior Analy...	11.0.0.0	[Gear] [Down Arrow]
Investigate Server	✓	NWAPPLIANCE8017	Investigate Server	11.0.0.0	[Gear] [Down Arrow]
Log Collector	✓	NWAPPLIANCE23030	Log Collector	11.0.0.0-14507.1.516...	[Gear] [Down Arrow]
Log Collector	✓	NWAPPLIANCE18419	Log Collector	11.0.0.0-14507.1.516...	[Gear] [Down Arrow]

At the bottom of the table, it says 'Page 1 of 1' and 'Displaying 1 - 25 of 25'. The footer of the interface shows 'RSA | NETWITNESS SUITE' and the version '11.0.0.0-170703005427.1.be97632'.

Administrators who feel comfortable working outside of the user interface can configure the basic parameters as well as advanced settings by editing database nodes in the Decoder node tree using the Services Explore view.

The screenshot shows the 'SERVICES' tab with the 'Decoder' service selected. The 'Explore' view is open, displaying a tree view on the left with 'Decoder (DECODER)' expanded. The 'config' folder is selected, showing a list of configuration parameters and their values.


Parameter	Value
aggregate.precache	on
assembler.parse.valve	false
assembler.pool.ratio	70
assembler.session.flush	1
assembler.session.pool	250000
assembler.size.max	32 MB
assembler.size.min	0
assembler.tcp.close	false
assembler.timeout.packet	60
assembler.timeout.session	60
assembler.voting.weights	first=1 size=1 port=1 octet=1 routable=1
capture.autostart	off
capture.buffer.size	64 MB
capture.device.params	
capture.selected	packet_mmap_lo
export.cache.expire	60
export.packet.enabled	no
export.packet.local.path	/var/netwitness/decoder/export/packet
export.packet.max	0

The footer of the interface shows 'RSA | NETWITNESS SUITE' and the version '11.0.0.0-170620070817.1.94259'.

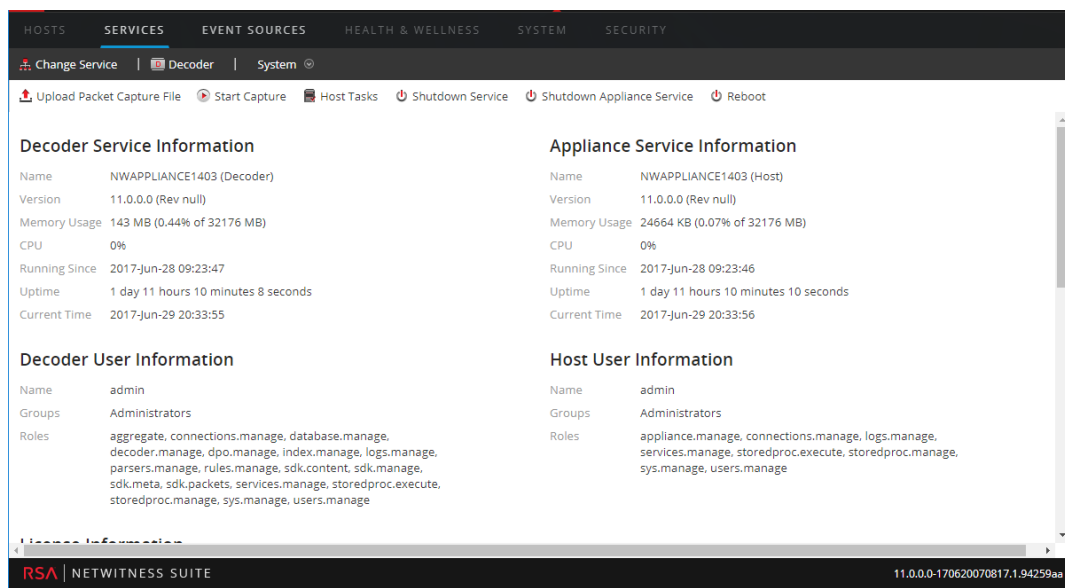
## Perform Initial Quick Setup

This procedure accomplishes the initial, basic configuration of a Decoder, and starts data capture. When the basic setup is complete, the Decoder begins capturing data for the Concentrator to consume.

To configure a Decoder and start capturing data:

1. Assign a network interface for capturing data. For details, see "Select a Network Adapter" in [Configure Capture Settings](#).
2. Do one of the following:
  - a. To start capture, select the Decoder and  > **View > System**. In the toolbar click

 **Start Capture**



The screenshot shows the RSA NetWitness Suite interface with the 'SERVICES' tab selected. The 'Decoder' service is highlighted in the left sidebar. The main content area displays two panels: 'Decoder Service Information' and 'Appliance Service Information'. Both panels show details for 'NWAPPLIANCE1403 (Decoder)' and 'NWAPPLIANCE1403 (Host)' respectively, including version, memory usage, CPU, and uptime. Below these are 'Decoder User Information' and 'Host User Information' panels, both showing 'admin' as the user and 'Administrators' as the group. The bottom of the interface shows the 'RSA | NETWITNESS SUITE' logo and the version '11.0.0.0-170620070817.1.94259aa'.

Decoder Service Information		Appliance Service Information	
Name	NWAPPLIANCE1403 (Decoder)	Name	NWAPPLIANCE1403 (Host)
Version	11.0.0.0 (Rev null)	Version	11.0.0.0 (Rev null)
Memory Usage	143 MB (0.44% of 32176 MB)	Memory Usage	24664 KB (0.07% of 32176 MB)
CPU	0%	CPU	0%
Running Since	2017-Jun-28 09:23:47	Running Since	2017-Jun-28 09:23:46
Uptime	1 day 11 hours 10 minutes 8 seconds	Uptime	1 day 11 hours 10 minutes 10 seconds
Current Time	2017-Jun-29 20:33:55	Current Time	2017-Jun-29 20:33:56

Decoder User Information		Host User Information	
Name	admin	Name	admin
Groups	Administrators	Groups	Administrators
Roles	aggregate, connections.manage, database.manage, decoder.manage, dpo.manage, index.manage, logs.manage, parsers.manage, rules.manage, sdk.content, sdk.manage, sdk.meta, sdk.packets, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage	Roles	appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

- b. To enable Capture Autostart, see "Configure a Decoder to Begin Capturing Data Automatically" in [Configure Capture Settings](#).

The Decoder begins capturing data for consumption by a Concentrator. For additional configuration options, refer to [Configure Common Settings on a Decoder](#) and [Decoder and Log Decoder Additional Procedures](#)

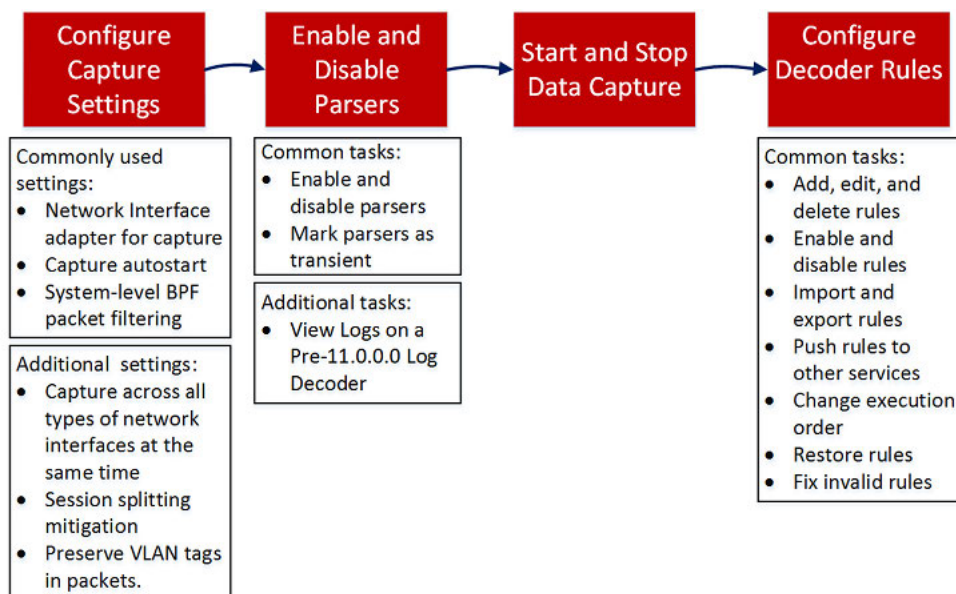


## Configure Common Settings on a Decoder

This section introduces commonly used configuration settings on a Decoder with procedures and background information. After you have completed [Decoder and Log Decoder Quick Setup](#), you can refine your configuration by using parsers, feeds, and rules to limit the captured data.

**Note:** A Log Decoder is a special type of Decoder, which is configured and managed in a similar way to a Decoder. Most of the information in this guide refers to both types of Decoders. "Decoder" refers to both types of Decoders. Information that applies exclusively to Packet Decoders or Log Decoders is clearly identified.

The following workflow illustrates commonly used settings and breaks the configuration process into four steps.

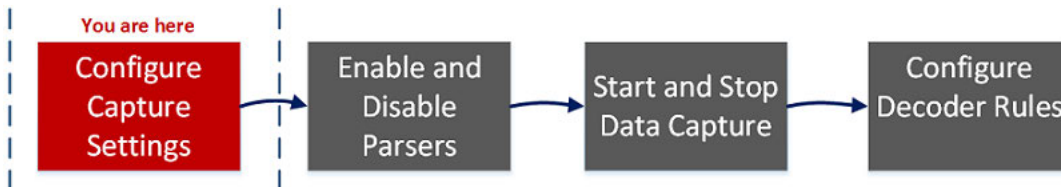


Configuration Step	Description
<a href="#">Configure Capture Settings</a>	When initially setting up the Decoder, configuring the network adapter interface is required. Additional optional capture settings are available; one that is frequently used is Capture Autostart.
<a href="#">Enable and Disable Parsers and Log Parsers</a>	View the parsers that have been downloaded and deployed from Live, and manage which ones are enabled or disabled.

Configuration Step	Description
<a href="#">Start and Stop Data Capture</a>	When a Decoder starts up, it automatically begins aggregating data if Capture Autostart is enabled. When autostart is not enabled, you can start and stop data capture manually.
<a href="#">Configure Decoder Rules</a>	<p>Capture rules can add alerts or contextual information to sessions or logs. They can also define which data a Decoder or Log Decoder filters out.</p> <p>By default, no capture rules are defined when you first configure NetWitness Suite. Unless rules are specified and the rules are valid, the packets are not filtered. You can deploy the latest rules from Live as described in the <i>Live Services Management Guide</i>. You can define capture rules at any time, and you can fix rules that use invalid syntax (<a href="#">Fix Rules with Invalid Syntax</a>).</p>

## Configure Capture Settings

When initially setting up the Decoder, configuring the network adapter interface is required. Additional optional capture settings are available; two that are frequently used are the Berkeley Packet Filter, and Capture Autostart.



Besides the basic network adapter interface setup, you may decide to use one of the special-purpose configurations described in [\(Optional\) Preserve VLAN Tags When Using the Packet MMAP Capture Interface](#) or [\(Optional\) Configure a Decoder to Capture Data Across All Types of Network Interfaces](#)

The rest of the capture settings have default values chosen to be effective in most cases (see a detailed list in [Services Config View - General Tab](#)). You can adjust these in some circumstances, for example, if Customer Support advises a change. You can edit the capture settings at any time.

## Select a Network Adapter

The table below describes the Network Adapter settings for a Decoder. The system administrator sets the default network adapters when the Decoder is installed. Consult your System Administrator for more information.


Adapter Parameter	Description
<b>Berkley Packet Filter</b>	Berkeley Packet Filters (BPF) are applied to the packet stream before the packets are copied to the Decoder adapter for analysis. This allows unwanted traffic to be efficiently discarded. However, any packets discarded are not accounted for in any Decoder statistics (capture rate, packets dropped, and packets filtered and total packets).

Adapter Parameter	Description
<b>Capture Interface Selected</b>	<p>Select an adapter through which the Decoder captures packets. For the lower speed internal capture interface, use the <code>packet_mmap_,7,eth1</code> adapter, which corresponds to the monitor port located on the motherboard. There are six additional capture ports:</p> <ul style="list-style-type: none"> <li>• <code>packet_mmap_,1,lo</code> (bpf)</li> <li>• <code>packet_mmap_,2,eth2</code> (bpf)</li> <li>• <code>packet_mmap_,3,eth3</code> (bpf)</li> <li>• <code>packet_mmap_,4,eth4</code> (bpf)</li> <li>• <code>packet_mmap_,5,eth5</code> (bpf)</li> <li>• <code>packet_mmap_,8,ALL</code> (bpf)</li> </ul> <p>There are three wireless capture services available:</p> <ul style="list-style-type: none"> <li>• <code>packet_netmon_</code> (Microsoft Netmon)</li> <li>• <code>packet_mac80211_</code> (Linux mac80211)</li> <li>• <code>packet_airport_</code> (Mac OS X AirPort)</li> </ul>
<b>Capture Interface Selected for Log Decoder</b>	<p>The following capture service is available:</p> <ul style="list-style-type: none"> <li>• <code>log_events</code>, Log Events</li> </ul>


#### To configure the network adapter on a Decoder:

1. Go to **ADMIN > Services**.




- In the **Administration Services** view, select the Decoder and  > **View > Config**.  
The Services Config view is displayed with the General tab open.


Decoder Configuration	
Name	Config Value
<b>Adapter</b>	
Berkeley Packet Filter	
Capture Interface Selected	packet_mmap_lo
<b>Cache</b>	
Cache Directory	/var/netwitness/decoder/cache
Cache Size	4 GB
<b>Capture Settings</b>	

- In the **Capture Interface Selected** field, select the network adapter that best suits the Decoder.
- To save the changes, click **Apply**.
- If necessary to put the changes into effect, navigate back up to the **Administration Services** view, select the Decoder, and select  > **Restart**.


## Configure a Decoder to Begin Capturing Data Automatically

- Go to **ADMIN > Services**.
- In the **Administration Services** view, select the Decoder and  > **View > Config**.  
The Services Config view is displayed with the General tab open

Decoder Configuration	
Name	Config Value
<b>Adapter</b>	
Berkeley Packet Filter	
Capture Interface Selected	packet_mmap_lo
<b>Cache</b>	
Cache Directory	/var/netwitness/decoder/cache
Cache Size	4 GB
<b>Capture Settings</b>	

- Under **Capture Settings**, select the **Capture Autostart** checkbox.
- To save the changes, click **Apply**.
- If necessary to put the changes into effect, navigate back up to the **Administration Services** view, select the Decoder, and select  > **Restart**.

## Configure Optional Capture Settings

1. Go to **ADMIN > Services**.
2. In the **Administration Services** view, select the Decoder and  > **View > Config**.  
The Services Config view is displayed with the General tab open.

### Decoder Configuration

Name	Config Value
<b>Adapter</b>	
Berkeley Packet Filter	
Capture Interface Selected	packet_mmap_lo
<b>Cache</b>	
Cache Directory	/var/netwitness/decoder/cache
Cache Size	4 GB
<b>Capture Settings</b>	

### Decoder Configuration

Name	Config Value
Parse Threads	0
<b>Database Max File Sizes</b>	
Meta File Size	auto
Packet File Size	auto
Session File Size	auto
<b>Hash</b>	
Hash Directory	

3. If you want to apply a system-level filter to the packet stream before the packets are copied to the Decoder adapter for analysis, configure the Berkeley Packet Filter as described in [\(Optional\) Configure System-Level \(BPF\) Packet Filtering](#).
4. In the **Capture Settings** sections, review the default values. When a service is first added, default values are in effect and should be changed only in special circumstances, for example, if Customer Support advises a change. See [Services Config View - General Tab](#) for an explanation of these settings.
5. In the **Database Max File Sizes** section, review the default values. When a service is first added, default values are in effect and should be changed only in special circumstances, for example, if Customer Support advises a change. See [Services Config View - General Tab](#) for an explanation of these settings.

6. In the **Hash** section, define a directory for hash files if you are using this feature. See [Services Config View - General Tab](#) for an explanation of these settings.

### **(Optional) Configure System-Level (BPF) Packet Filtering**

You can use Berkeley Packet Filters to control which packets and logs are processed by a Decoder.

Berkeley Packet Filters (BPF) are applied to the packet stream before the packets are copied to the Decoder adapter for analysis. This allows unwanted traffic to be efficiently discarded. These discarded packets are not accounted for in any Decoder statistics (capture rate, packets dropped, and packets filtered and total packets).

The Decoder also supports system-level packet filtering defined using `tcpdump/libpcap` syntax. Specifying a `Libpcap` filter can efficiently reduce packet volume based on Layer 2 - Layer 4 attributes. A `Libpcap` filter is appropriate for use when a Decoder is receiving a traffic volume that is placing a load against the physical resources of the platform. In this scenario, the Decoder may consistently drop packets and have a large number of capture pages available (`/decoder/stats/capture.pagefree` is high).

The following is an example of a `libpcap` filter to keep only packets that do not have both source and destination addresses in the 10.21.0.0/16 subnet.


```
not (src net 10.21.0.0/16 and dst net 10.21.0.0/16)
```

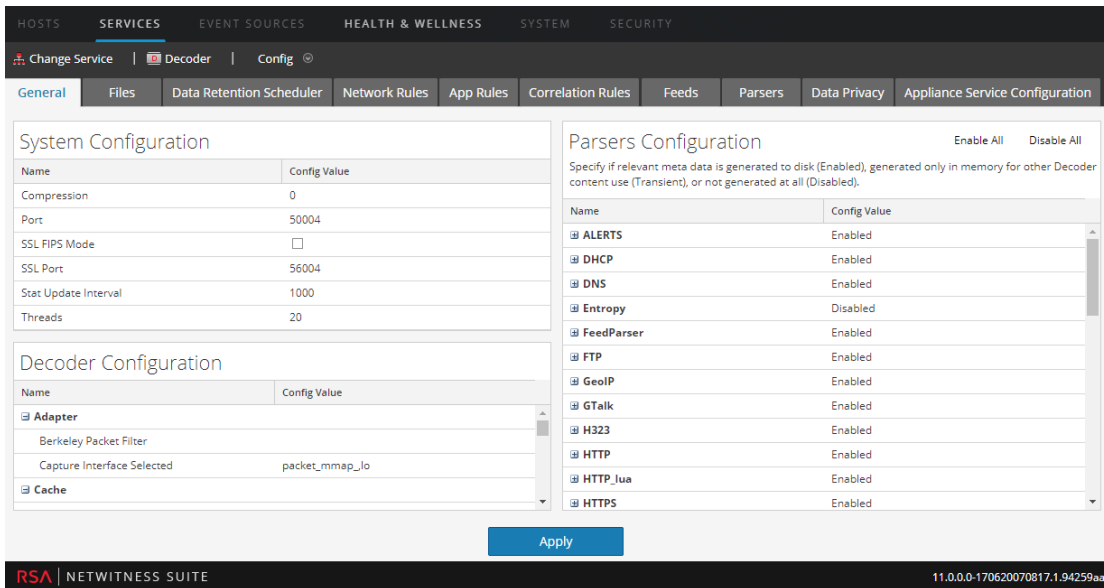
For a full reference of the `Libpcap` filter syntax, see the main pages for:

- `tcpdump` ([http://www.tcpdump.org/tcpdump\\_man.html](http://www.tcpdump.org/tcpdump_man.html)).
- `pcap-filter` (<http://www.unix.com/man-page/FreeBSD/7/pcap-filter/>).

#### **To add a system-level Berkeley Packet Filter:**

1. Go to ADMIN > **Services**.

- In the Administration Services view, select a Decoder service and  > **View > Config**.  
The Services Config view is displayed with the General tab open.



The screenshot shows the RSA NetWitness Suite configuration interface. The top navigation bar includes tabs for HOSTS, SERVICES, EVENT SOURCES, HEALTH & WELLNESS, SYSTEM, and SECURITY. The 'SERVICES' tab is active, and the 'Config' sub-tab is selected. Below the navigation bar, there are several tabs: General, Files, Data Retention Scheduler, Network Rules, App Rules, Correlation Rules, Feeds, Parsers, Data Privacy, and Appliance Service Configuration. The 'General' tab is currently open.

The 'General' tab contains two main sections: 'System Configuration' and 'Decoder Configuration'. The 'System Configuration' section has a table with the following data:

Name	Config Value
Compression	0
Port	50004
SSL FIPS Mode	<input type="checkbox"/>
SSL Port	56004
Stat Update Interval	1000
Threads	20

The 'Decoder Configuration' section has a table with the following data:

Name	Config Value
Adapter	Berkeley Packet Filter
Capture Interface Selected	packet_mmap_lo
Cache	

The 'Parsers Configuration' section on the right has a table with the following data:

Name	Config Value
ALERTS	Enabled
DHCP	Enabled
DNS	Enabled
Entropy	Disabled
FeedParser	Enabled
FTP	Enabled
GeoIP	Enabled
GTalk	Enabled
H323	Enabled
HTTP	Enabled
HTTP_lua	Enabled
HTTPS	Enabled

At the bottom of the configuration page, there is an 'Apply' button. The footer of the page shows 'RSA | NETWITNESS SUITE' and the version '11.0.0.0-170620070817.1.94259aa'.

- In the **Decoder Configuration Section**, under **Adapter**, click in the field next to **Berkeley Packet Filter**.
- Type only one filter in the field. If you want to filter multiple items, join multiple expressions using **and**. Several examples are provided below.  
The user interface validates input at the time you enter your filter string.
- To save the filter, click **Apply**.  
If the syntax is correct, a confirmation message is displayed.  
If the syntax is incorrect, a **Packet filter is not valid** message is displayed and a corresponding log message will follow in the log messages on the Decoder:  

```
164474800      2015-May-01 19:03:08      warning      Decoder      Failed
to parse filter 'example_badrule': syntax error
```
- To activate the filter, you must stop and start capture on the Decoder:
  - Change the **Config** view to the **System** view.
  - Click **Stop Capture**.
  - Click **Start Capture**.
The active filter will be displayed in the Decoder logs.

## Examples

These are several filter examples:

- Drop packets to or from any address in the 10.21.0.0/16 subnet:  
`not (net 10.21.0.0/16)`
- Drop packets that have both source and destination addresses in the 10.21.0.0/16 subnet:  
`not (src net 10.21.0.0/16 and dst net 10.21.0.0/16)`
- Drop packets that are from 10.21.1.2 or are headed to 10.21.1.3.  
`not (src host 10.21.1.2 or dst host 10.21.1.3)`
- Combine both IP and HOST:  
`not (host 192.168.1.10) and not (host api.wxbug.net)`
- Drop all port 53 traffic, both TCP & UDP:  
`not (port 53)`
- Drop only UDP port 53 traffic:  
`not (udp port 53)`
- Drop all IP protocol 50 (IPSEC) traffic:  
`not (ip proto 50)`
- Drop all traffic on TCP ports 133 through 135.  
`not (tcp portrange 133-135)`

The following filters combine some of the above to demonstrate how to put multiple directives into one filter:

- Drop any port 53(DNS) traffic sourced from 10.21.1.2 or destined to 10.21.1.3.  
`not (port 53) and not (src host 10.21.1.2 or dst host 10.21.1.3)`
- Drop any traffic using IP proto 50 or port 53 or any traffic from net 10.21.0.0/16 destined to net 10.21.0.0/16  
`not (ip proto 50 or port 53) or not (src net 10.21.0.0/16 and dst net 10.21.0.0/16)`

**Caution:** The use of parentheses can have a large and potentially disruptive effect on the use of Packet Filters. As a best practice, keep "not" operations outside of parentheses and always test your rules before deploying them. Failure to properly format your rules (despite input validation) can cause a packet filter to drop ALL traffic or behave in other unexpected ways. This is due to the way packet Libpcap filters work and is not the result of any logic within NetWitness Suite software.

### Testing

BPF filters can and should be tested using either `tcpdump` or `windump` to ensure that they will provide the expected behavior before implementing them. This example shows a test of a filter using `windump`:

```
windump -nni 2 not (port 53 or port 443) or not (ip proto 50)
```

## Conversions

If for the sake of performance, you have decided that an existing network rule filter would be better running as a System-Level Packet Filter, you can convert it. There are a few things to remember when doing conversions.

- `&&` becomes `and`
- `ip.addr` becomes `host` if a single host or `net` if a network.
- `ip.src` becomes `src host` if a single host or `src net` if a network.
- `ip.dst` becomes `dst host` if a single host or `dst net` if a network.
- Use CIDR notation when listing a network (that is, `10.10.10.0/24`).
- `||` becomes `or`
- `!` becomes `not`
- Multiple rules must be joined with `and`.

The manual for TCPDump also gives examples of filters and strings that can be used:

[http://www.tcpdump.org/tcpdump\\_man.html](http://www.tcpdump.org/tcpdump_man.html)

Additionally, the following site provides an excellent reference for BPF-style packet filters:

<http://biot.com/capstats/bpf.html>

**Caution:** If you are capturing `vlan` tagged packets, above standard bpf filter may not work. For example, if you use `not (udp port 123)` to filter `vlan` tagged NTP traffic on `udp port 123`, it will not work. This is because the bpf filter machinery is simple and does not account for protocols not referenced in the rule. So the OS executing the bpf filter will look for the `udp port` values at the byte offset they would occur in a standard Ethernet/udp packet; but the optional `vlan` tag fields in the Ethernet header pushes those values by 4 bytes, thus the bpf filter rule will fail. To fix it, you need to change the bpf filter to: `not (vlan and udp port 123)`.

## (Optional) Configure a Decoder to Capture Data Across All Types of Network Interfaces

The `packet_mmap_,ALL` adapter is capable of capturing across all types of network interfaces at the same time. For example, this can include things like physical network interfaces over different media types and tunnel interfaces.


The default behavior of the ALL adapter is to capture from all interfaces from the system, except for the hard-coded defaults of `lo`, `eth0`, and `em1`.

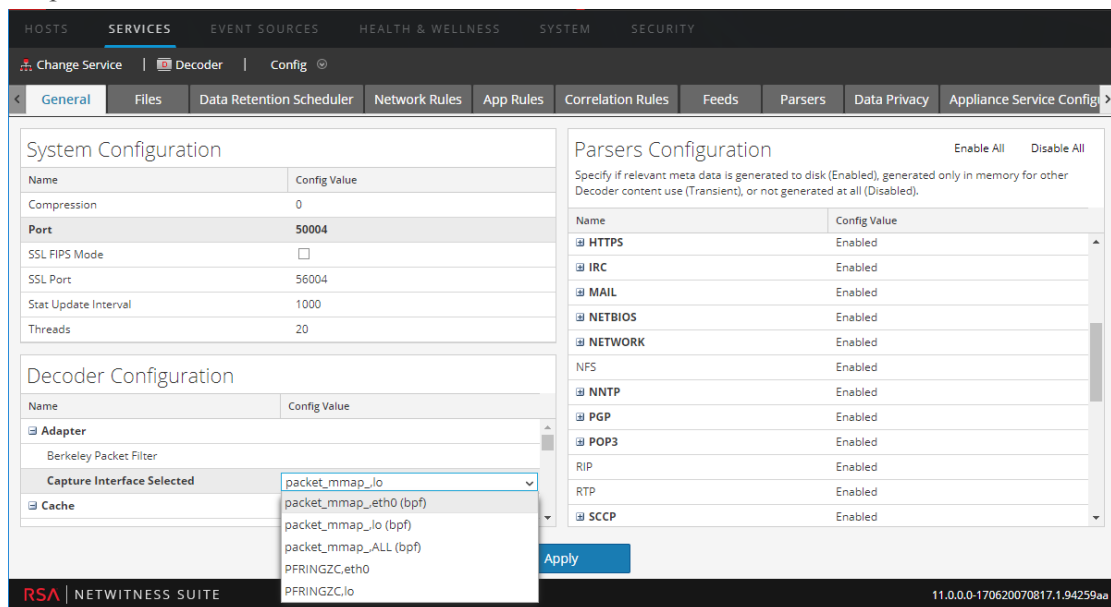
In NetWitness Suite 11.0, you can select any subset of the capture interfaces by editing the Decoder configuration node `/decoder/config/capture.device.params` to include an `interfaces=` parameter. The `interfaces` parameter contains a comma-separated list of interfaces that are used for capture. Instead of using all interfaces for capture, only the specified interfaces are used.

For example, if you want to force capture on interfaces `em1`, `em2`, and `em4`, and ignore `em3`, you can select the `packet_mmap_`, ALL adapter, and then add this line to `capture.device.params: interfaces=em1, em2, em4`

**Note:** Using the `interfaces` parameter to select `eth0`, `lo`, or `em1` overrides the default behavior, which is to drop traffic from those ports.

### To configure the `packet_mmap_`, ALL adapter to capture from specific interfaces instead of all interfaces:

1. In the **Administration Services** view, select the Decoder service and  > **View** > **Config**.
2. In the **Services Config** view, set **Capture Interface Selected** to `packet_mmap_`, ALL adapter.



3. To go to the Services Explore view, click **Config** in the toolbar and select **Explore** in the drop-down list.

4. In the Services Explore view, select **decoder > config**.

Parameter	Value
aggregate.precache	on
assembler.parse.valve	false
assembler.pool.ratio	70
assembler.session.flush	1
assembler.session.pool	250000
assembler.size.max	32 MB
assembler.size.min	0
assembler.tcp.close	false
assembler.timeout.packet	60
assembler.timeout.session	60
assembler.voting.weights	first=1 size=1 port=1 octet=1 routable=1
capture.autostart	off
capture.buffer.size	64 MB
capture.device.params	
capture.selected	packet_mmap_lo
export.cache.expire	60
export.packet.enabled	no
export.packet.local.path	/var/netwitness/decoder/export/packet
export.packet.max	0

5. Click in the values column next to `capture.device.params`, type `interfaces=em1,em2,em4`, and press **Enter**.

Parameter	Value
assembler.session.pool	250000
assembler.size.max	32 MB
assembler.size.min	0
assembler.tcp.close	false
assembler.timeout.packet	60
assembler.timeout.session	60
assembler.voting.weights	first=1 size=1 port=1 octet=1 routable=1
capture.autostart	off
capture.buffer.size	64 MB
capture.device.params	interfaces=em1,em2,em4
capture.selected	packet_mmap_lo
export.cache.expire	60
export.packet.enabled	no
export.packet.local.path	/var/netwitness/decoder/export/packet
export.packet.max	0
export.packet.remote.path	/var/netwitness/decoder/export/packet
export.packet.size.max	1 GB
export.session.enabled	no
export.session.format	avro

The change goes into effect immediately; only traffic on `em1`, `em2`, and `em4` interfaces is captured.



## (Optional) Preserve VLAN Tags When Using the Packet MMAP Capture Interface

When capturing traffic containing VLAN tags, you may need to configure the Packet MMAP capture interface to preserve the VLAN tags in the packets (VLAN fixup). By default, the network capture hardware removes the tags. Performing this procedure preserves the tags in the packets, and the tag values are parsed into VLAN meta data for further analysis.

There are two mechanisms for enabling the VLAN fixup.

- Option 1: Set `vlan-fix=true` within `capture.device.params`. This option performs the VLAN fixup on all traffic entering the Decoder. This option is appropriate in most cases, since it is assumed that all the traffic will be VLAN tagged. This mechanism works on either single-interface mode, or on all-interfaces mode. This option overrides the VLAN fixup settings on individual interfaces; even interfaces that are not configured to do VLAN fixup will have the feature enabled.
- Option 2: Use the `interfaces` parameter within `capture.device.params` on a per-device basis. The `interfaces` parameter accepts a comma-separated list of interface names on which to capture packets. By adding `:vlan` to an interface name, you can enable the VLAN fixup on individual interfaces. If the interface does not have the `:vlan` suffix added, then it will not perform the VLAN fixup.


After editing this parameter, you must restart capture on the Decoder in order for changes to `capture.device.params` to take effect.

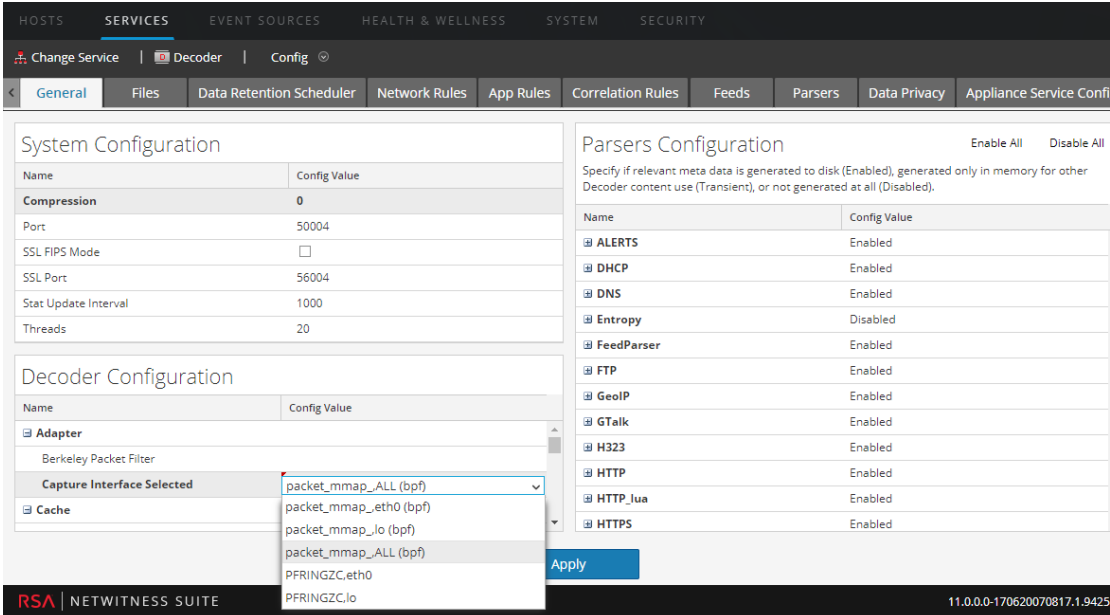
These are `vlan` examples of both options. If you need to pass multiple settings for `capture.device.params`, use the following syntax. Notice that quotes are needed for values with whitespace, see *Core Database Tuning Guide*.

```
name1="value1" name2="value2".
```

Parameter	Value	Effect
<code>capture.device.params</code>	<code>vlan-fix=true</code>	VLAN fixup always performed on all interfaces. The default value is <code>vlan-fix=false</code> .
<code>capture.device.params</code>	<code>interfaces=eth0:vlan,eth1</code>	VLAN fixup performed on traffic capture on <code>eth0</code> interface only
<code>capture.device.params</code>	<code>interfaces=eth0:vlan,eth1</code> <code>vlan-fix=true</code>	VLAN fixup always performed because the <code>vlan-fix</code> setting overrides the <code>interfaces</code> setting.

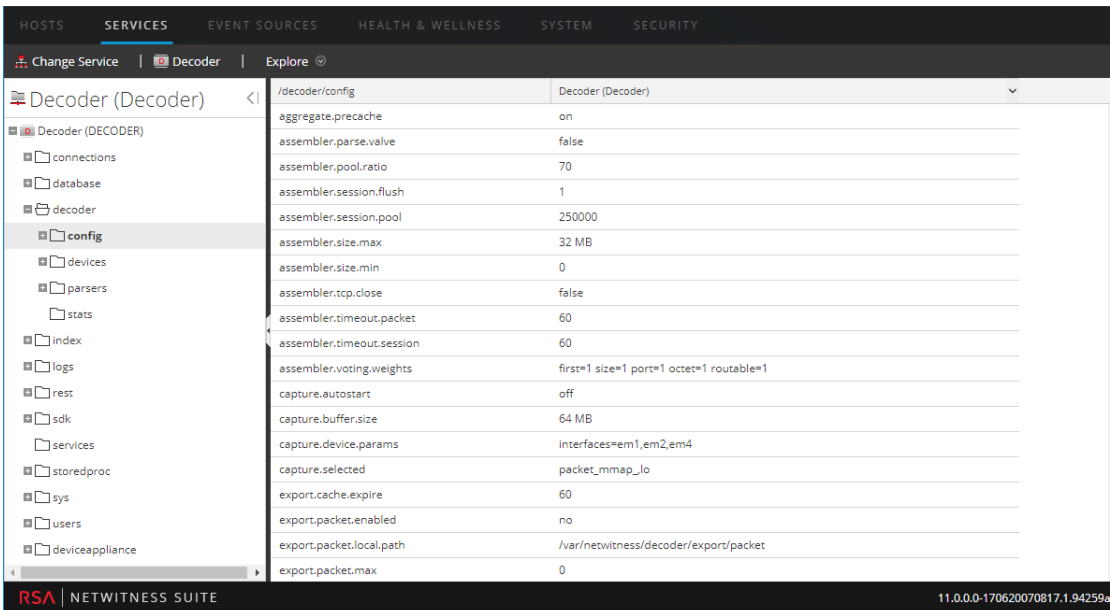
### To configure the `packet_mmap_adapter` to preserve the VLAN tags in packets:

1. In the **Administration Services** view, select the Decoder service and  > **View** > **Config**.
2. In the **Services Config** view, set **Capture Interface Selected** to `packet_mmap_`, ALL adapter.



The screenshot shows the 'Config' view for the Decoder service. The 'General' tab is selected, displaying 'System Configuration' and 'Decoder Configuration'. In the 'Decoder Configuration' section, the 'Capture Interface Selected' dropdown is open, showing options like 'packet\_mmap\_ALL (bpf)', 'packet\_mmap\_eth0 (bpf)', and 'PFRINGZC.eth0'. The 'Parsers Configuration' section on the right lists various parsers such as ALERTS, DHCP, DNS, and HTTP, all of which are enabled.

3. To go to the Services Explore view, click **Config** in the toolbar and select **Explore** in the drop-down list.
4. In the Services Explore view select **decoder** > **config**.



The screenshot shows the 'Explore' view for the Decoder service. The 'config' section is expanded, displaying a list of configuration parameters and their values. The 'capture.selected' parameter is set to 'packet\_mmap\_lo'. Other parameters include 'aggregate.precache' (on), 'assembler.parse.valve' (false), 'assembler.pool.ratio' (70), 'assembler.session.flush' (1), 'assembler.session.pool' (250000), 'assembler.size.max' (32 MB), 'assembler.size.min' (0), 'assembler.tcp.close' (false), 'assembler.timeout.packet' (60), 'assembler.timeout.session' (60), 'assembler.voting.weights' (first=1 size=1 port=1 octet=1 routable=1), 'capture.autostart' (off), 'capture.buffer.size' (64 MB), 'capture.device.params' (interfaces=em1,em2,em4), 'export.cache.expire' (60), 'export.packet.enabled' (no), 'export.packet.local.path' (/var/netwitness/decoder/export/packet), and 'export.packet.max' (0).

5. Click in the values column next to `capture.device.params`, and do one of the following:

- To preserve VLAN tags on an interface in the interfaces list, add `:vlan` after the interface name and press **Enter**. For example, this specifies that VLAN tags are preserved on `em1`, but not on `em2` and `em4`:

`interfaces=em1:vlan,em2,em4`

Parameter	Value
assembler.session.pool	250000
assembler.size.max	32 MB
assembler.size.min	0
assembler.tcp.close	false
assembler.timeout.packet	60
assembler.timeout.session	60
assembler.voting.weights	first=1 size=1 port=1 octet=1 routable=1
capture.autostart	off
capture.buffer.size	64 MB
<b>capture.device.params</b>	<b>interfaces=em1:vlan,em2,em4</b>
capture.selected	packet_mmap_lo
export.cache.expire	60
export.packet.enabled	no
export.packet.local.path	/var/netwitness/decoder/export/packet
export.packet.max	0
export.packet.remote.path	/var/netwitness/decoder/export/packet
export.packet.size.max	1 GB
export.session.enabled	no
export.session.format	json

The change goes into effect immediately; only traffic on `em1` has the VLAN tags preserved.

- To preserve VLAN tags on all interfaces, enter the following and press **Enter**:

`vlan-fix=true`.

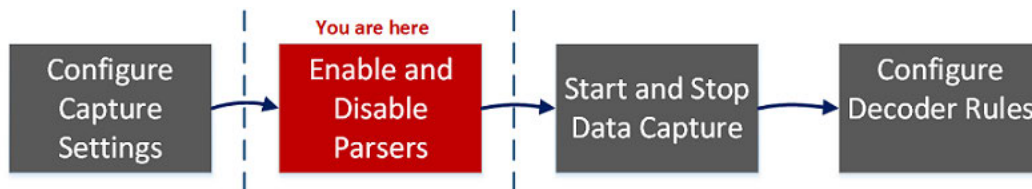
Parameter	Value
aggregate.precache	on
assembler.parse.valve	false
assembler.pool.ratio	70
assembler.session.flush	1
assembler.session.pool	250000
assembler.size.max	32 MB
assembler.size.min	0
assembler.tcp.close	false
assembler.timeout.packet	60
assembler.timeout.session	60
assembler.voting.weights	first=1 size=1 port=1 octet=1 routable=1
capture.autostart	off
capture.buffer.size	64 MB
<b>capture.device.params</b>	<b>vlan-fix=true</b>
capture.selected	packet_mmap_lo
export.cache.expire	60
export.packet.enabled	no
export.packet.local.path	/var/netwitness/decoder/export/packet
export.packet.max	0

The change goes into effect immediately; VLAN tags are preserved on all capture interfaces.

## Enable and Disable Parsers and Log Parsers

Administrators can see which parsers have been downloaded from Live and deployed on a Decoder or Log Decoder, see which of these have been enabled, and enable or disable parsers and log parsers.

The following figure illustrates commonly used settings on a Decoder. For a quick basic setup with only the required steps, see [Decoder and Log Decoder Quick Setup](#).



You should only download and deploy the parsers you need for the following reasons:

- There is an impact on performance as you increase the number of deployed parsers.
- The more parsers you deploy, the more meta data created, which impacts data retention
- Not having extra (unnecessary) log parsers deployed reduces the potential for misidentification of messages.


The Parsers Configuration panel provides a way to select parsers to use on the Decoder. Within some parsers, you can also configure the metadata that the parser creates. These are the options in the Parsers Configuration panel.

Option	Description
<b>Enable</b>	These options provide a way to quickly select either all parsers or no parsers.
<b>All</b>	
<b>Disable</b>	
<b>All</b>	
<b>Name</b>	The names of parsers available to the Decoder. A plus sign indicates that the metadata generated by the parser is configurable. Clicking the plus sign displays the metadata that the parser can create.

Option	Description
<b>Config Value</b>	<p>A drop-down list changes the setting for the parser or metadata to <b>Enabled</b>, <b>Disabled</b>, or <b>Transient</b>.</p> <ul style="list-style-type: none"> <li>When <b>Enabled</b>, the Decoder is using the parser to filter traffic.</li> <li>When <b>Transient</b>, the Decoder is using the parser to filter traffic, and the generated metadata is not stored on disk. The transient metadata is available in memory to additional content (that is, parsers, feeds, and application rules) on that Decoder. This helps administrators to protect certain data and is usually done as part of a data privacy plan (see the <i>Data Privacy Management Guide</i>).</li> <li>When <b>Disabled</b>, the Decoder is not using the parser.</li> </ul> <p>If the generated metadata for the parser is configurable, clicking the plus sign to expand the parser displays configurable meta keys and the same drop-down list selects the meta key the parser will create.</p>

**Note:** For a Log Decoder You must have previously deployed log parsers from Live, See the **Find and Deploy Live Resources** topic in the *Live Services Management Guide* for details. Go to the [Master Table of Contents](#) for Version 11.0 to find NetWitness Suite 11.0 documents.

**To enable or disable an parser, or to view the status for each parser:**

1. Go to **ADMIN > Services**.
2. In the **Administration Services view**, select a Log Decoder or a Decoder, and  >**View > Config**.

3. In the **Parsers Configuration** panel, look for the Decoder parser or the Log Decoder event source parser.

**Parsers Configuration** Enable All Disable All

Specify if relevant meta data is generated to disk (Enabled), generated only in memory for other Decoder content use (Transient), or not generated at all (Disabled).

Name	Config Value
<b>ALERTS</b>	Enabled
alert	Enabled
DHCP	Disabled
DNS	Transient
Entropy	Enabled
FeedParser	Enabled
FTP	Enabled
GeoIP	Enabled
GTalk	Enabled
H323	Enabled
HTTP	Enabled
HTTP_lua	Enabled
HTTPS	Enabled
IRC	Enabled
MAIL	Enabled

4. In the **Config Value** column, note the current status for your parser.

You can update the status of any individual parser by selecting its **Config Value** and selecting **Disabled**, **Transient**, or **Enabled** from the drop-down menu. Alternatively, you can select **Enable All** or **Disable All** to update the status for all of your log parsers at once.

5. Click **Apply**.

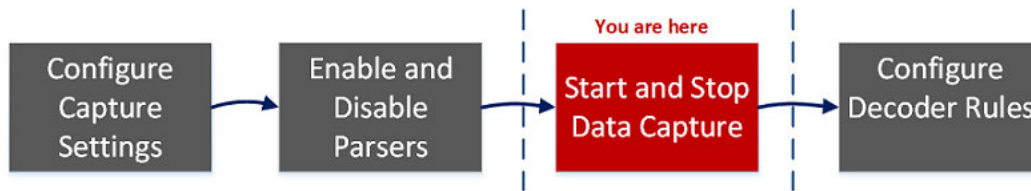
When you click **Apply**, note that all parsers are reloaded into NetWitness Suite. The status for each parser is updated, based on your selections.

## Start and Stop Data Capture



When a Decoder starts up, it automatically begins aggregating data if **Capture Autostart** is enabled. When autostart is not enabled, you can start and stop data capture manually.

**Note:** The Capture Configuration Settings in the Service Config view for a Decoder determine whether Capture Autostart is enabled.

The following figure illustrates commonly used settings on a Decoder. For a quick basic setup with only the required steps, see [Decoder and Log Decoder Quick Setup](#). You may want to stop and start capture at other times, for example, before you shut down the service.



### To start and stop capture:

1. Go to **ADMIN > Services**.
2. In the **Admin Services** view, select a Decoder or Log Decoder service, and select   **> View > System**.
3. In the toolbar, click **Start Capture**.  
If the service is a Decoder, it begins capturing packets. If the service is a Log Decoder, it begins capturing logs.  
When packet or log capture is in progress, the option in the toolbar changes to **Stop Capture**, and the option to upload a file is unavailable.
4. Whenever you want to discontinue traffic capture on a Decoder, click **Stop Capture**.  
Packet or log capture ceases, and the option to upload a file to the service is again available.

**Note:** When you stop the Log Decoder service while capture is running, all events currently in Log Decoder memory will be processed and persisted. Should an issue arise where it is necessary to quickly shutdown the service, use the Services Explore view to stop capture (**/decoder stop**), passing the parameters *flush=false* before stopping the Log Decoder service. For further information, see the "Services Explore View" in the *Host and Services Getting Started Guide*.

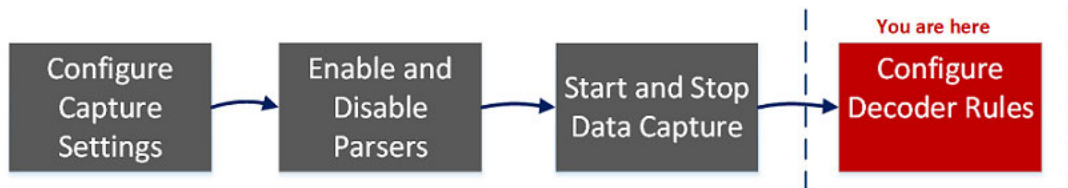


## Configure Decoder Rules

---

This topic provides procedures for creating and managing rules for Decoder or Log Decoder traffic capture in the Services Config view > Rules tabs . [Services Config View - Rules Tabs](#) provides details about the Rules tab options.

The following figure illustrates commonly used settings on a Decoder. For a quick basic setup with only the required steps, see [Decoder and Log Decoder Quick Setup](#).



Capture rules can add alerts or contextual information to sessions or logs. They can also define which data is filtered out by a Decoder or Log Decoder. Rules are created for specific metadata patterns, which result in predefined actions when matches are found. For example, to keep all traffic that fits certain criteria, but discard all other traffic, you can create a rule to perform the necessary actions. When applied, rules affect both packet capture file importing, as well as live network capture.

[Rule and Query Guidelines](#) provides guidelines that all queries and rule conditions in NetWitness Suite Core Services must follow.

By default, no rules are defined when you first install NetWitness Suite. Until rules are specified, the packets are not filtered. You can deploy the latest rules from Live. You can define three types of rules: Network Rules, Application Rules, and Correlation Rules.

- Network rules are applied at the packet level and are made up of rule sets from Layer 2, Layer 3, and Layer 4. Multiple rules can be applied to the Decoder. Rules can be applied to multiple layers (for example, when a network rule filters out specific ports for a specific IP address). Network rules are only available on packet Decoders.
- Application rules are applied at the session level. If the first rule listed is not a match, the Decoder then attempts to match the next rule listed, until a match is found.
- Correlation rules are applied over a configurable sliding time window. When a match is found, the service creates a new super session that identifies other sessions that match the rule, then creates a session list for analysis.

The two most common uses of rules are:

- To alert, and thereby create a custom alert meta value, when certain conditions are found.
- To filter out certain types of traffic that do not add value to the analysis of the data.

Groups of capture rules form rule sets, which you can import and export. This feature enables use of multiple rule sets for various scenarios. You can import the exported rule set, in the form of an .nwr file, to other NetWitness Suite services, simplifying the deployment and configuration of multiple services.

## Rule Processing

These are the principles governing capture rule processing:

- Multiple rules can be applied to the Decoder.
- Capture rules are executed one after the other, in sequence.
- Rule processing stops when all rules are processed or after a rule configured to stop rule processing is matched.
- A default rule can be used to either include or exclude all traffic not otherwise selected by a rule. A default rule, if used, must always be placed at the bottom of the rule list. Otherwise, rule processing stops as soon as the default rule is evaluated since, by definition, all traffic is selected by the default rule.
- When rule processing stops, the session is saved using the configured session options and debug options.

## Rule Configuration

### Rule and Query Guidelines

All queries and rule conditions in RSA NetWitness Core services must follow these guidelines:

**All string literals and time stamps must be quoted. Do not quote numbers, MAC, or IP addresses.**

- `extension = 'torrent'`
- `time='2015-jan-01 00:00:00'`
- `service=80`
- `ip.src = 192.168.0.1`

**Note:** The space on the right and the left of an operator is optional. For example, you can type a rule as `service=80` or `service = 80`.

## Rule Examples

The following table shows examples of rule conditions. You can use rule conditions for log retention collections in an Archiver and for application, network, and correlation rules on a Decoder, Log Decoder, or Concentrator. Rule conditions are also used in all `WHERE` clauses in all Core database queries.

For detailed information on rule syntax in NetWitness Suite, see "WHERE Clauses" in the "Queries" section of the *Core Database Tuning Guide*.

Rule Name	Condition
ComplianceDevices	<code>device.group='PCI Devices'    device.group='HIPPA Devices'</code>
HighValueWindows	<code>device.group='Windows Compliance'</code>
MediumValueWindows	<code>device.type='winevent_nic' &amp;&amp; msg.id='security_ 4624_security'</code>
LowValueWinLogs	<code>device.type='winevent_nic' &amp;&amp; msg.id='security_ 4648_security'</code>
LowValueProxyLogs	<code>device.class='proxy' &amp;&amp; msg.id='antivirus_ license_expired'</code>
GeneralWindows	<code>device.type='winevent_nic'</code>

## Invalid Rules

NetWitness Suite uses a rule parser that strictly defines valid syntax for rules and queries. When a Core service encounters invalid syntax, it writes a warning in the NetWitness Suite logs indicating the error.

**Note:** NetWitness Suite 11.0 does not support parsing of legacy syntax rules (as NetWitness Suite 10.6 did). After you update to NetWitness Suite 11.0, rules with invalid syntax are highlighted in the user interface, and no rules will be applied until the invalid rules are corrected. The Rule Editor provides additional tooltips. After you fix the rules, the highlights disappear. See [Fix Rules with Invalid Syntax](#).

The `/decoder/config/rules/rule.errors` and `/concentrator/config/rules/rule.errors` stats, contain the count of rules with errors. If `rule.errors` is nonzero, NetWitness Suite generates a Health and Wellness alert to indicate that you need to fix the rules.

## General Syntax Guidelines

- All text values must quote literal values. Example: `username = 'user1'`
- Quotes can use single or double quotes; but they must match. (You cannot start with a single quote and finish with a double quote.)
- If the literal value has a quote, you can escape it (using a backslash) or use a different starting quote character. Both of the following examples are valid: `username = "User's"`, `username = 'User\'s'`

The following are valid syntax rules:

- To use a backslash in a literal string, escape it using an extra backslash: `\`
- All time values should use quotes for dates in this form:  
`time = 'YYYY-MM-DD HH:MM:SS'`
- All time values that are the number of seconds since EPOCH (Jan 1, 1970), should not be quoted.  
Example: `time = 1448034064`
- **Everything** else is unquoted: IP addresses, MAC addresses, numerics, and so on. Example:  
`service = 80 && ip.src = 192.168.1.1/16`

## Capture Rule Syntax

Capture rules compare fields to values or to other fields. This is an example of a simple expression with a meta key on the left side of the operator and a value on the right side.

```
ip.dst=192.168.1.1
```

The syntax allows a meta key on the right side of the operator in Decoders and Log Decoders for application and network rules. Meta key comparison does not apply in the `where` clause in queries. This is an example of a simple expression with a meta key on the left side of the operator and a meta key on the right side.

```
ip.src=ip.dst
```

Rules that include a meta key comparison support renamed meta keys; if a rule queries a meta key that has been renamed, the rule is parsed for the renamed meta key. For example, if the meta key `ip_dst` is used in a rule, it is transparently mapped to the renamed meta key: `ip.dst`. Existing rules that include original keys will trigger alerts that include data for the renamed meta key. .

This is an example of a rule that finds packets having the same `ip.src` address and `ip.dst` address on a Decoder, and generates an alert on the Concentrator.

```
alert=alert.id name=testRule8 rule="ip.src=ip.dst" order=38
```

This rule would generate an error because `eth.src` and `ip.src` are incompatible formats.

```
rule="eth.src=ip.src" name="testRule99" alert=alert.id
```

Values can be expressed as discrete values, a range of values, an upper or lower bound, or a combination of these three. You can create a greater than or less than comparison, and test equality or inequality against a range of values or an upper/lower bound.

`key 0-5` (a range of values)

`key = 0-u` is the same as `key >= 0` (upper bound, greater than or equal to)

The following table summarizes the operators on meta keys.

Left Operand Format	Operator	Right Operand Format	Description
any	=	compatible with left operand	Equality operator. You can use values or meta keys on the right side of the equality operator.
any	!=	compatible with left operand	Inequality operator. You can use values or meta keys on the right side of the inequality operator.
any	<	compatible with left operand	Less than operator. You can use values or meta keys on the right side of this operator.
any	<=	compatible with left operand	Less than or equal to operator. You can use values or meta keys on the right side of this operator.
any	>	compatible with left operand	Greater than operator. You can use values or meta keys on the right side of this operator.

Left Operand Format	Operator	Right Operand Format	Description
any	<code>&gt;=</code>	compatible with left operand	Greater than or equal to operator. You can use values or meta keys on the right side of this operator.
text	<code>contains</code>	text	Find values that contain the right operand. You can use meta keys or values on the right side of this operator.
text	<code>begins</code>	text	Find values that begin with the right operand. You can use meta keys or values on the right side of this operator.
text	<code>ends</code>	text	Find values that end with the right operand. You can use meta keys or values on the right side of this operator.
text	<code>length</code>	integer	Find strings of a certain length. You can use meta keys or values on the right side of this operator.
any	<code>count</code>	integer	Find values with a specific number of occurrences within the session. You can use meta keys or values on the right side of this operator.
any	<code>ucount and unique</code>	integer	Finds a number of uniquely occurring values. You can use meta keys or values on the right side of this operator. For example, if the results include instances of a meta key with 5 unique values and 3 of the same value, the <code>ucount</code> is 6.
N/A	<code>exists</code>	any	Finds any values for the meta key. You can use meta keys or values on the right side of this operator.
N/A	<code>!exists</code>	any	Finds any sessions in which the meta key does not occur. You can use meta keys or values on the right side of this operator.

Left Operand Format	Operator	Right Operand Format	Description
text	regex	text	Finds values matching a regular expression. You can use values on the right side of this operator.

The following table summarizes other syntax elements used in rules.

Syntax element	Description
*	Default rule. By using an asterisk (*) as the sole character in a rule, that rule will select all traffic.
u	Upper bound of a range a range of times, IP addresses, or numeric formats. For example, to select all TCP ports above 40000, the syntax would be: <code>tcp.port = 40000-u</code>
l	Lower bound of a range of times, IP addresses, or numeric values. For example, to select all TCP ports below 40000, the syntax would be: <code>tcp.port = 1-40000</code>
- (dash)	Denotes a range. This is only applicable to time values, IP or MAC addresses, or numeric values. Separate the lower and upper bounds of the range with a dash (-) character. For example, to select TCP ports between 25 and 443, the syntax would be: <code>tcp.port = 25-443</code>
, (comma)	Denotes a list of ranges or values or meta keys. Single values may be used as well as any combination of ranges and upper or lower bounds. Single meta keys may be used in a list. Meta keys and literal values cannot both appear on the right-hand side of an operator. For example, the following is valid syntax: <code>tcp.port = 1-10,25,110,143-225,40000-u</code>


Syntax element	Description
( )	Grouping operator. An expression can be enclosed in parentheses to create a new logical expression. For example, the following would select traffic on port 80 to/from 192.168.1.1 OR traffic on port 443 to/from 10.10.10.1:  <code>(ip.addr=192.168.1.1 &amp;&amp; tcp.port=80)    (ip.addr=10.10.10.1 &amp;&amp; tcp.port=443)</code>
~	Logical NOT operator, a negation of an expression.
&&	Logical AND operator, a conjunction of two expressions.
	Logical OR operator, a disjunction of two expressions.

## Configure Capture Rules

The Decoder and Log Decoder rules are editable in the Services Config view. While each type of rule (network, application, and correlation) has its own tab; the functions are similar for all types of rules. You can:

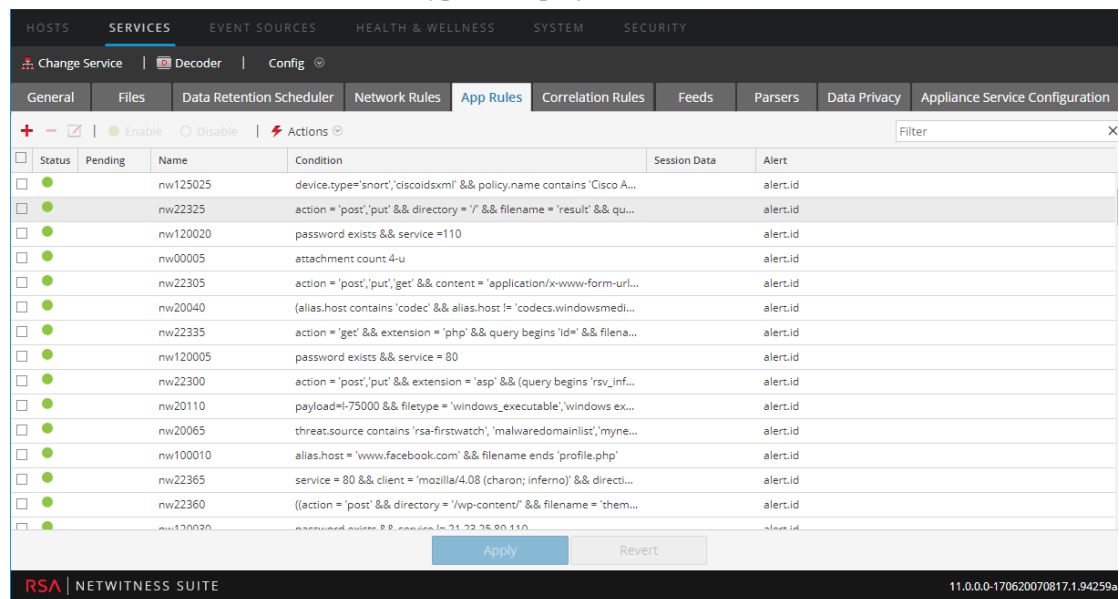
- Add, edit, and delete rules
- Enable and disable rules
- Change the execution sequence of rules
- Import rules from a file
- Export rules to a file
- Push rules to another service
- Revert or apply rule changes
- Restore one of the last ten rule configurations from a snapshot

### To configure rules in the Rules tabs

1. Go to **ADMIN > Services**.
2. In the **Services** view, select a Decoder service and  > **View > Config**.
3. In the **Services Config** view, select one of the Rules tabs: Network Rules, App Rules, or Correlation Rules.



The rules list for the selected rule type is displayed.




Each type of rule has a list with slightly different columns and different parameters. Several basic guidelines apply to all rule management activities:

- The rules are executed in the sequence they are displayed in the list. To change the execution sequence of rules, drag and drop rules to the appropriate location in the list or use the context menu options to arrange the rules in the list.
- To select a single row, click the row.
- To select a group of adjacent rows, click the first, then shift-click the row at the end of the group.
- To select multiple non-adjacent rows, click the first, then control-click the others.
- When editing rules in the Rules tab, you must apply the configuration changes in order to activate.
- Until changes are applied, you can discard edits to the list and revert to the unedited rules.
- Once rules are applied, you can recover the last ten rules configurations using the **History** option in the **Actions** menu.

**To add a rule in any Rules tab, do one of the following:**


- Click **+**.
  - Right-click a rule, and select **Insert Above** or **Insert Below** from the context menu.
- The Rule Editor dialog for that type of rule is displayed.

**To remove a rule:**

1. From any Rules tab, select the rules to remove from the rules list.
2. Click .


The selected rules are removed from the list, but still exist on the service.

**To edit a rule**

1. From any Rules tab, select the rule to edit.
2. Click  or double-click the rule row.


The Rule Editor dialog for that type of rule is displayed.

**To disable a rule:**

1. From any Rules tab, select the rules to disable.
2. Click  Disable.

The status changes to disabled in the rules list, but the rule is still enabled on the service.

**To enable a rule:**

1. From any Rules tab, select the rules to enable.
2. Click  Enable.

The status changes to enabled in the rules list, but the rule is still disabled on the service.

## Import Rules from a File and Export Rules

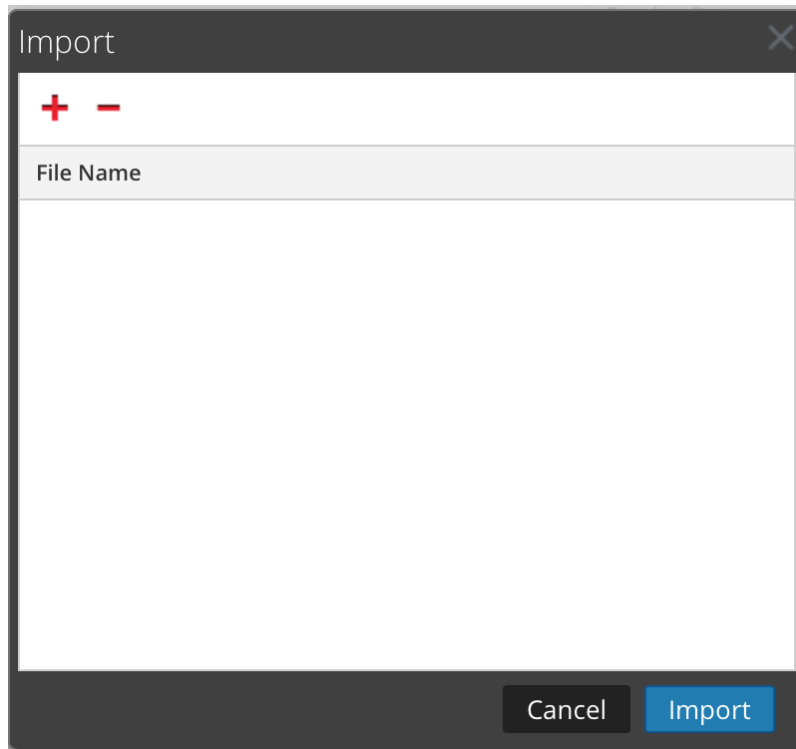
You can import network, application, and correlation rules to a Decoder from a file that contains rules of the same type. After the rules are imported, you can edit and manage them as you would any other rules.

When you attempt to import a group of rules, NetWitness Suite Administration checks the type of rules imported. If you are successful, a message displays the number of rules imported. If the rule type differs from the active tab type, the rules are not imported. You must re-import the rules under the correct tab or select another file to import.

**To import rules to a service:**

1. From any Rules tab, select  Actions   Import.

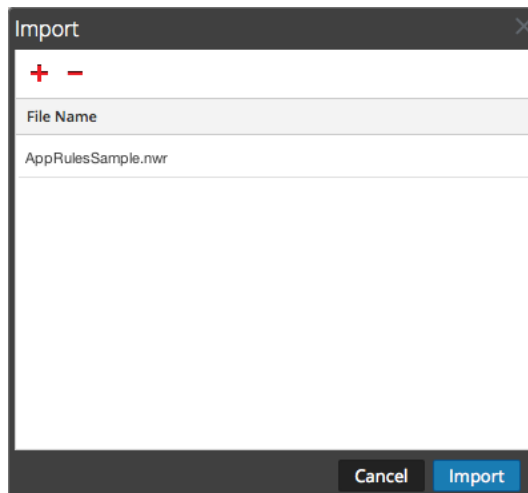
The Import dialog is displayed.



2. Click **+**.

A view of the directory structure is displayed.

3. Choose one or more NetWitness rules (.nwr) files to import, and click **Open**.  
The file is added to the list in the Import dialog.




4. Click **Import**.

The rules are imported into the user interface. Imported rules have a red corner in each edited column.

5. Edit or reorder the rules if needed.

6. To save the rules to the service, click **Apply**.  
The rules for the service are updated with the changes.


#### To export a rule to a file:

1. To export a subset of the rules, select the rules to be exported.
2. Do one of the following:
  - In the toolbar, select  **Actions** ▾ > **Export** > **Selection**. (**Export** > **All** exports all rules in the rules list even if you have a subset selected for export.)
  - Right-click the selected rules and select **Export Selection**.  
A prompt for the filename is displayed.
3. Enter the filename and click **Export**.  
The **.nwr** file is downloaded.

## Push Rules to Other Services

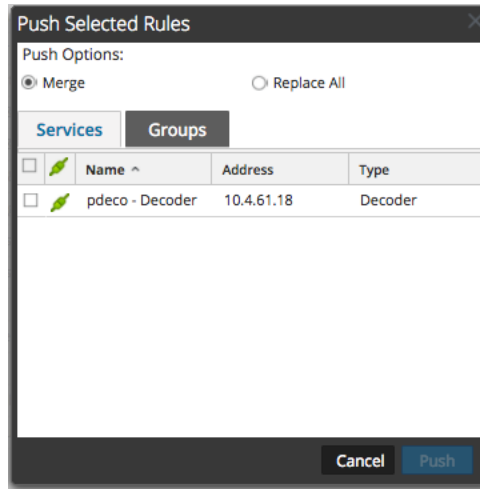
You can apply (push) rules or selected rules to other services (Decoders or Log Decoders) or service groups. When you push all rules to other services, all rules on the target services are removed and replaced with all of the rules on the source service.

#### To push selected rules from this Decoder to other Decoders:

1. From any Rules tab, select the rules that you want to push to another Decoder.
2. Do one of the following:
  - Select  **Actions** ▾ > **Push** > **Selection**.

- Right-click the selected rules and select **Push Selected Rules**.


The Push Selected Rules dialog is displayed.

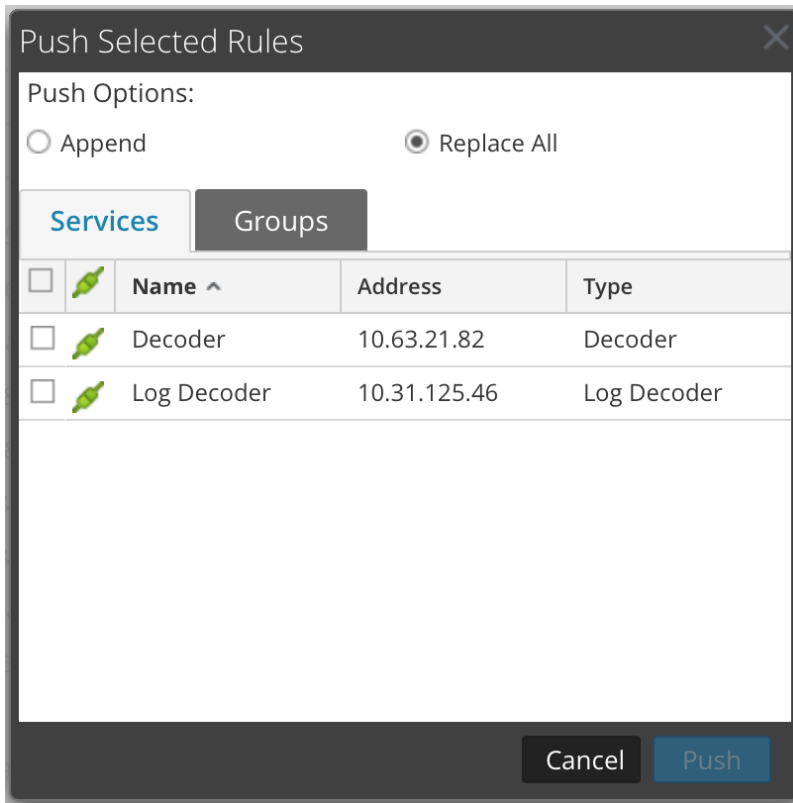


3. Select a Push Option:
  - Select **Replace All** to delete all rules on the target services and replace them with the selected rules. This is the default selection.
  - Select **Merge** to merge the selected rules with the existing rules on the target services.
4. On the **Services** tab, select the target services to receive the pushed rules, or select the groups of services from the **Groups** tab.
5. Click **Push**.

The rules are pushed to the selected services and become effective immediately.

#### To push all rules from this Decoder to other Decoders:

1. From any Rules tab, select  **Actions** > **Push** > **All**.  
(**Push** > **All** pushes all rules in the rules list even if you have a subset selected to push.) The Push Selected Rules dialog is displayed.



2. On the **Services** tab, select the target services to receive the pushed rules, or select the groups of services from the **Groups** tab.
3. Click **Push**.  
All rules from the target services are deleted and replaced with all of the rules from source service. The rules become effective immediately.

## Change Execution Order of Rules


Capture rules are applied in the order they are displayed in the rules list. To reorder rules, use either of these methods:

- Drag and drop the rules in the appropriate location in the rules list.
- Right-click a rule to display the context menu, and use the **Cut** and **Paste** options.

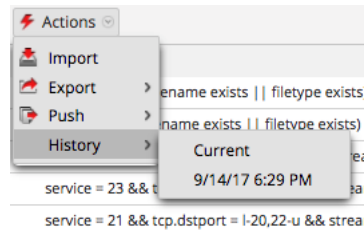
## Restore a Rule Snapshot from History

NetWitness Suite keeps the last ten snapshots of rules applied to a service.

### To restore a rules snapshot from history:

1. Select  **Actions** > **History**.

A submenu of snapshots is displayed.



2. Select the snapshot time from the submenu.

The rules from the snapshot are loaded into the rules list, replacing the current set. But the current set is still in use on the service.

3. To apply the rules to the service, click **Apply**.

The rules are applied to the service.

## Configure Application Rules

Application layer rules are applied at the session level. The following are sample application rules.

To truncate packets carried via Server Message Block protocol (SMB), create a rule as follows:

- Rule Name: Truncate SMB
- Condition: `service=139`
- Rule Action: Truncate

To retain email to and from a specific e-mail address, create a rule as follows:

- Rule Name: Email Filter Tom Jones
- Condition: `email='Tom.Jones@TheShop.com'`
- Rule Action: Filter

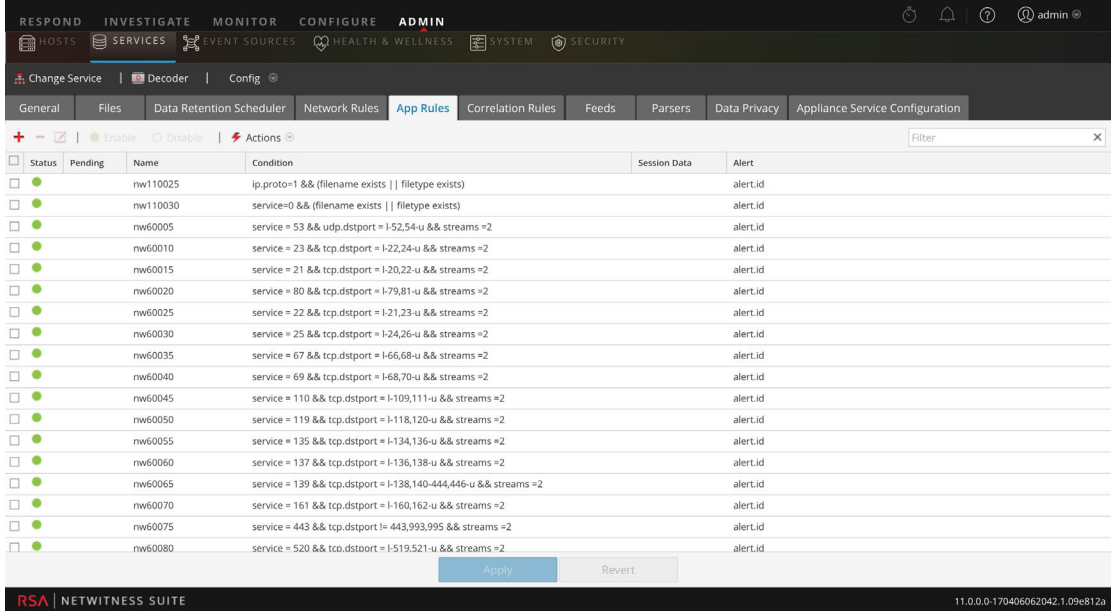


### To add or edit an application rule:

1. Go to **ADMIN > Services**.
2. Select a Decoder or Log Decoder service and  > **View > Config**.

The Systems Config view for the selected service is displayed.

3. Select the **App Rules** tab.



Status	Pending	Name	Condition	Session Data	Alert
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw110025	ip.proto=1 && (filename exists    filetype exists)		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw110030	service=0 && (filename exists    filetype exists)		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60005	service = 53 && udp.dstport = 1-52,54-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60010	service = 23 && tcp.dstport = 1-22,24-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60015	service = 21 && tcp.dstport = 1-20,22-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60020	service = 80 && tcp.dstport = 1-79,81-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60025	service = 22 && tcp.dstport = 1-21,23-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60030	service = 25 && tcp.dstport = 1-24,26-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60035	service = 67 && tcp.dstport = 1-66,68-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60040	service = 69 && tcp.dstport = 1-68,70-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60045	service = 110 && tcp.dstport = 1-109,111-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60050	service = 119 && tcp.dstport = 1-118,120-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60055	service = 135 && tcp.dstport = 1-134,136-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60060	service = 137 && tcp.dstport = 1-136,138-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60065	service = 139 && tcp.dstport = 1-138,140-444,446-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60070	service = 161 && tcp.dstport = 1-160,162-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60075	service = 443 && tcp.dstport != 443,993,995 && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60080	service = 520 && tcp.dstport = 1-519,521-u && streams =2		alert.id

4. Do one of the following:

If adding a new rule, click .

If editing a rule, select the rule from the rules list and click .

5. The Rule Editor Dialog is displayed with application rule parameters.

**Rule Editor**

**Rule Definition**

Rule Name:

Condition:

*All string literals and time stamps must be quoted.  
Do not quote number values and ip addresses.  
[Examples] : 1. device.group='Windows Compliance' && service = 443  
2. time = '2015-jan-01 00:00:00' - u  
3. ip.src = 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16 || extension = 'torrent'*

**Session Data**

☒ Stop Rule Processing

☐ Keep

☐ Filter

☒ Truncate

**Session Options**

☒ Alert ☐ Forward ☐ Transient

Alert On

**Reset** **Cancel** **OK**

- In the **Rule Name** field, type a name for the rule. For example, for a rule that truncates all SMB, type **Truncate SMB**.
- In the **Condition** field, build the rule condition that triggers an action when matched. You can type directly in the field or build the condition in this field using meta from the window actions. As you build the rule definition, NetWitness Suite displays syntax errors and warnings. For example, to truncate all SMB, type **service=139**.  
All string literals and time stamps must be quoted. Do not quote number values and IP addresses. [Configure Decoder Rules](#) provides additional details.
- If you want rule evaluation to end with this rule, check the **Stop Rule Processing** checkbox.
- In the **Session Data** section, choose one of the following actions to apply when a matching packet is found:
 

**Keep:** The packet payload and associated meta are saved when they match the rule.

**Filter:** The packet is not saved when it matches the rule.

**Truncate:** The packet payload is not saved when it matches the rule, but packet headers and associated meta are retained.

- e. In the **Session Options** section, do any of the following:
  - **To generate a custom alert** when a session metadata matches the rule, enable the Alert flag and select the name of the alert meta from the **Alert On** drop-down list.
  - **To perform syslog forwarding** when the log matches the rule, enable the **Forward** flag. Make sure that:
    - You have enabled both the Alert and Forward flags to carry out syslog forwarding.
    - The name of the rule mentioned in the Rule Editor dialog matches the syslog forwarding destination name specified in the Log Decoder > View > Explore > /decoder/config/logs.forwarding.destination parameter
  - **To prevent the alert metadata that is created from being written to the disk**, enable the **Transient** flag.
6. To save the rule and add it to the grid, click **OK**.

The rule is added at the end of the grid or inserted where you specified in the context menu. The plus sign is displayed in the **Pending** column.
7. Check that the rule is in the correct execution sequence with other rules in the grid. If necessary, move the rule.
8. To apply the updated rule set to the Decoder or Log Decoder, click **Apply**.

NetWitness Suite saves a snapshot of the currently applied rules, then applies the updated set to the Decoder and removes the pending indicator from the rules that were pending.

## Configure Correlation Rules

Basic Correlation Rules are applied at the session level and alert the user to specific activities that may be occurring in their environment. NetWitness Suite applies correlation rules over a configurable sliding time window. When the conditions are met, alert metadata is created for this activity and there is a visible indicator of the suspicious activity.

The following are sample correlation rules illustrating two use cases and the syntax.

Objective: In sessions where `tcp.dstport` exists, if there is any combination of `ip.src` and `ip.dst` where the count of unique instances of `tcp.dstport` > 5 within 1 minute, then alert. To achieve this objective, create a rule as follows:

- Rule Name: IPv6 Vertical TCP Port Scan 5
- Rule: `tcp.dstport exists`
- Instance Key: `ip.src,ip.dst`
- Threshold: `u_count(tcp.dstport)>5`
- Time Window: 1 min

Objective: In sessions where `action==login` and `error==fail`, if there is any combination of `ip.src` and `ip.dst` that appears in more than 10 sessions within 5 minutes, then alert. To achieve this objective, create a rule as follows:


- Rule Name: IPv4 Potential Brute Force 10
- Rule: `action='login' && error='fail'`
- Instance Key: `ip.src,ip.dst`
- Threshold: `count()>10`
- Time window: 5 mins

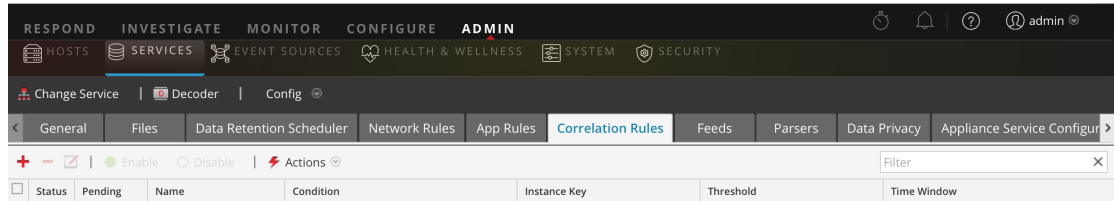
Both sample rules have the same instance key: `ip.src` and `ip.dst`. Because we are looking for unique combinations of `ip.src` and `ip.dst` that match the correlation condition, **`ip.src`** and **`ip.dst`** are **primary keys**.

Threshold can include an **associated key** that identifies the meta type that we are counting to determine if the condition is satisfied. In the first example, the associated key specified in Threshold is `tcp.dstport`. We are counting unique instances of `tcp.dstport` for every `ip.src/ip.dst` pair. In the second example, the associated key is not specified in the Threshold because it is merely a count of sessions. It is helpful to think of this scenario as counting unique session IDs and the associated meta is implicitly `session.id`. We are counting unique `session.id` for every `ip.src/ip.dst` pair.

**Invalid use case:** In sessions where (rule), if there is any combination of `ip.src` and `ip.dst` that have a unique count of `ipv6.dst > 5` within (time window), then alert. This case does not work because the associated key `ipv6.dst` is an IPv6 meta type. IPv4 and IPv6 meta types are not permitted to be used as associated keys.

### To add or edit a correlation rule

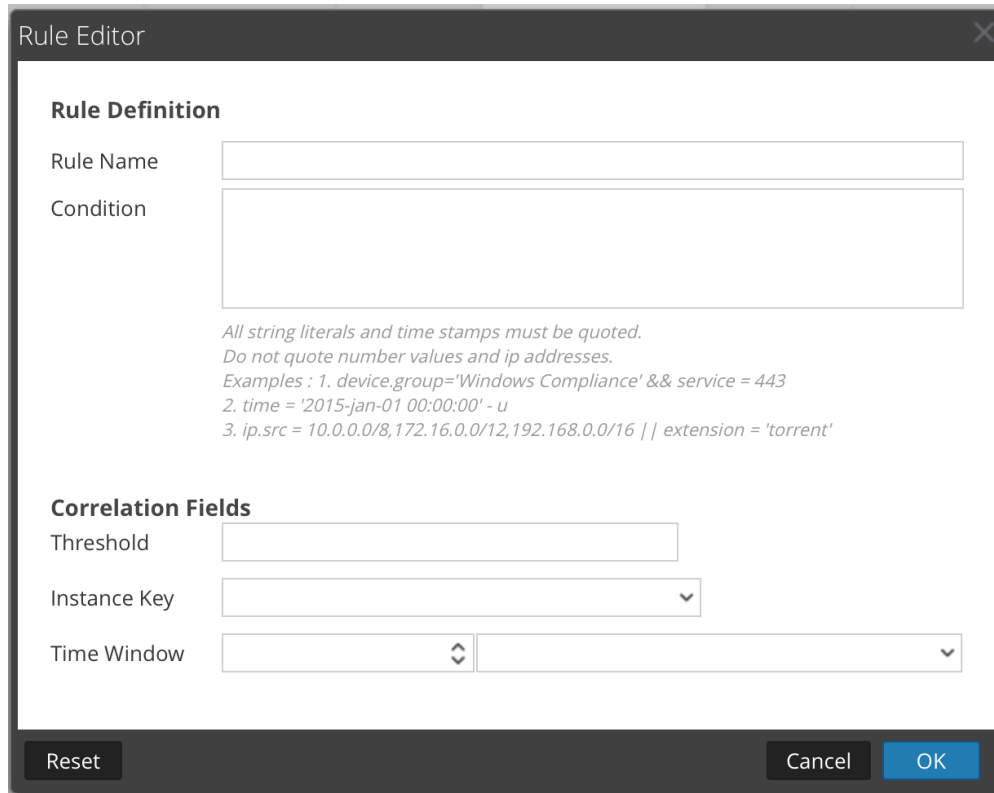
1. Go to **ADMIN > Services**, select a service, and  > **View > Config**.  
The Service Config view for the selected service is displayed.
2. Select the **Correlation Rules** tab.



3. In the **Correlation Rules** tab, do one of the following:
  - If adding a new rule, click .

- If editing a rule, select the rule from the rules grid and click .

The Rule Editor dialog is displayed with correlation rule parameters.



**Rule Editor**

**Rule Definition**

Rule Name

Condition

*All string literals and time stamps must be quoted.  
Do not quote number values and ip addresses.  
Examples : 1. device.group='Windows Compliance' && service = 443  
2. time = '2015-jan-01 00:00:00' - u  
3. ip.src = 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16 || extension = 'torrent'*

**Correlation Fields**

Threshold

Instance Key

Time Window

Reset Cancel OK

4. In the **Rule Name** field, type a name for the rule. For example, to create the sample rule, **IPv6 Vertical TCP Port Scan 5**.
5. In the **Condition** field, build the rule condition that triggers an action when matched. You can type directly in the field or build the condition in this field using meta from the window actions. As you build the rule definition, syntax errors and warnings are displayed by NetWitness Suite. For example, to create the sample rule, type **tcp.dstport exists**. When this condition is matched, the session data action is performed.  
All string literals and time stamps must be quoted. Do not quote number values and IP addresses. [Configure Decoder Rules](#) provides additional details.
6. In the **Threshold** field, use one of the threshold parameters to specify the minimum number of occurrences required to create a correlation session and an associated key if required. The associated key cannot be an IPv4 or IPv6 meta type.
  - `u_count(associated_key)` = the count of unique values of the specified key
  - `sum(associated_key)` = the values of the specified key
  - `count` = number of sessions (no associated key is specified)

7. In the **Instance Key** field, select the target indicator to base the event upon. This can be a single key or a compound key (two primary keys, separated by a comma).
8. In the **Time Window**, set the duration during which the threshold must be reached to create a correlation session.
9. To save the rule and add it to the grid, click **OK**.  
The rule is added at the end of the grid or inserted where you specified in the context menu.  
The plus sign is displayed in the **Pending** column.
10. Check that the rule is in the correct execution sequence with other rules in the grid. If necessary, move the rule.
11. To apply the updated rule set to the service, click **Apply**.  
NetWitness Suite saves a snapshot of the currently applied rules, then applies the updated set to the Decoder or Log Decoder.

## Configure Network Rules

Network rules are applied at the packet level on a Decoder and are made up of rule sets from Layer 2, Layer 3, and Layer 4. Multiple rules can be applied at the packet level to a Decoder. Network rules can apply to multiple network layers (for example, when a network rule filters out specific ports for a specific IP address). Network rules do not apply to Log Decoders, they apply only to packet Decoders.

You can create and manage network rules in the Services Config view > Network Rules tab.

### Supported Meta Keys in Network Rule Conditions

The following table describes the meta keys that NetWitness Suite supports for use in network rule conditions.

Meta Key	Description
<code>eth.addr</code>	Ethernet source or destination address. Commonly known as the MAC address.
<code>eth.dst</code>	Destination Ethernet address. This is the same as the Ethernet address field except that it selects only packets where the destination address matches the selected value(s).
<code>eth.src</code>	Same as Ethernet destination except that it focuses on the source address.
<code>eth.type</code>	Ethernet frame type.
<code>hdlc.type</code>	Frame type of the HDLC frame.
<code>ip.addr</code>	IPv4 source or destination address in standard form. IP addresses can be entered in CIDR notation for subnets.
<code>ip.dst</code>	Destination IPv4 address in standard form. IP addresses can be entered in CIDR notation for subnets.
<code>ip.proto</code>	IPv4 protocol field.
<code>ip.src</code>	Source IPv4 address in standard form. IP addresses can be entered in CIDR notation for subnets.



Meta Key	Description
<code>ipv6.addr</code>	IPv6 source or destination address in hex format. Generally IPv6 addresses are written as eight groups of four hex digits, thus expressing the entire 128 bit address length. Supports notation to represent multiple blocks of 0000 in an address. Does not support CIDR notation.
<code>ipv6.dst</code>	Destination IPv6 address in hex format.
<code>ipv6.proto</code>	IPv6 protocol field. This maps to the Next Header field in the IPv6 header and uses the same values as the IPv4 protocol field.
<code>ipv6.src</code>	Source IPv6 address in hex format.
<code>tcp.dstport</code>	Destination TCP port.
<code>tcp.port</code>	TCP source or destination port.
<code>tcp.srcport</code>	Source TCP port.
<code>udp.dstport</code>	Destination UDP port.
<code>udp.port</code>	UDP source or destination port.
<code>udp.srcport</code>	Source UDP port.

The following are sample network rules.

To truncate all SSL from the source port, create a rule as follows:

- Rule Name: Truncate SSL
- Condition: `tcp.srcport=443`
- Rule Action: Truncate

To filter subnet traffic, create a rule as follows:

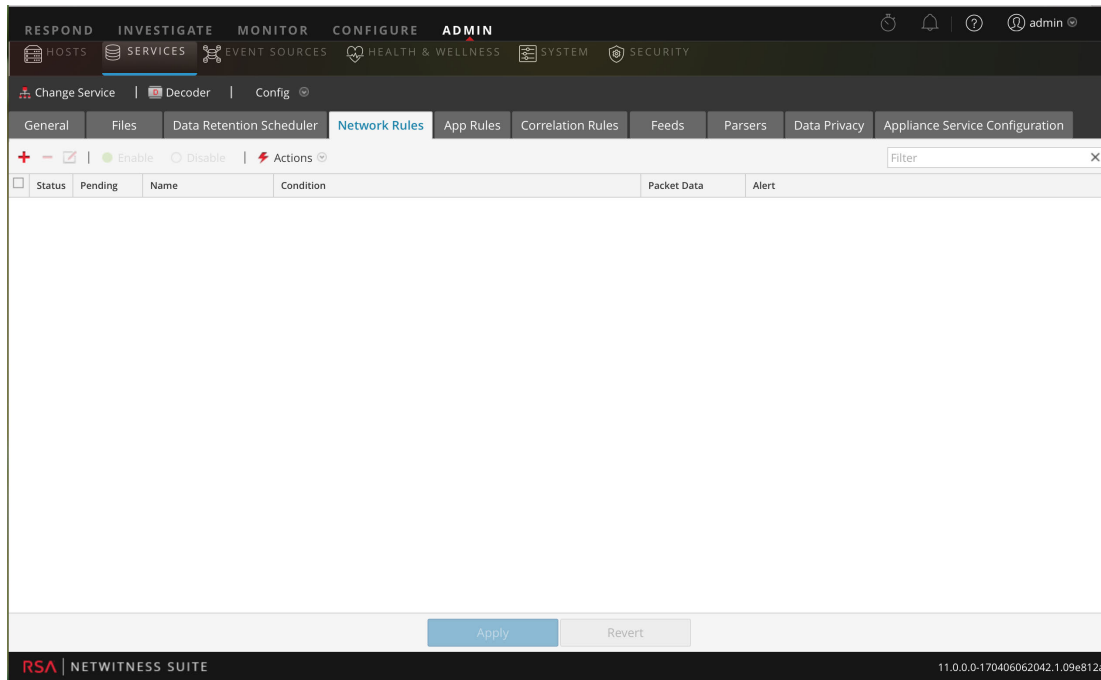
- Rule Name: Subnet Filter
- Condition: `ip.addr=192.168.2.0/24`
- Rule Action: Filter


**To add or edit a network rule:**

1. Go to **ADMIN > Services**, select a Decoder service, and  > **View > Config**.  
The Services Config view for the selected service is displayed.

2. Select the **Network Rules** tab.

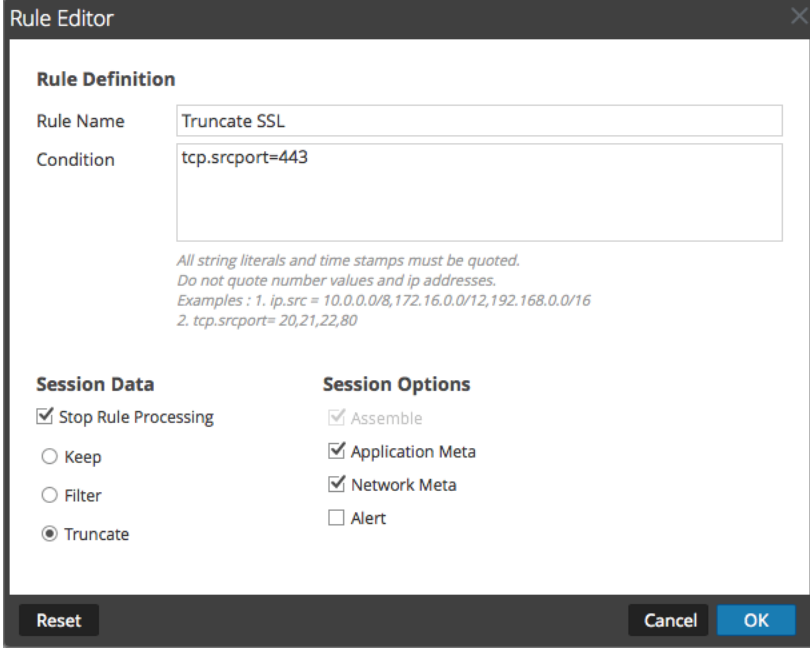
The Network Rules tab is displayed.



3. In the **Network Rules** tab, do one of the following:
  - If adding a new rule, click .

- If editing a rule, select the rule from the rules list and click .

The Rule Editor dialog is displayed.



**Rule Editor**

**Rule Definition**

Rule Name: Truncate SSL

Condition: tcp.srcport=443

*All string literals and time stamps must be quoted.  
Do not quote number values and ip addresses.  
Examples : 1. ip.src = 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16  
2. tcp.srcport= 20,21,22,80*

**Session Data**

☒ Stop Rule Processing

☐ Keep

☐ Filter

☒ Truncate

**Session Options**

☒ Assemble

☒ Application Meta

☒ Network Meta

☐ Alert

Reset Cancel OK


4. In the **Rule Name** field, provide a name for the rule. For example, for a rule that truncates all SSL from the source port, type **SSL Truncate**.
5. In the **Condition** field, build the rule condition that triggers an action when matched. You can type directly in the field or build the condition in this field using meta from the window actions. As you build the rule definition, NetWitness Suite displays syntax errors and warnings. For example, to truncate all SSL from the source port, **tcp.srcport=443**.  
All string literals and time stamps must be quoted. Do not quote number values and IP addresses. [Configure Decoder Rules](#) provides additional details. [Supported Meta Keys in Network Rule Conditions](#) describes the meta keys that NetWitness Suite supports for use in network rule conditions.
6. If you want rule evaluation to end with this rule, select the **Stop Rule Processing** checkbox.
7. In the **Session Data** section, choose one of the following actions to apply when a matching packet is found:
  - **Keep**: The packet payload and associated meta are saved when they match the rule.
  - **Filter**: The packet is not saved when it matches the rule.
  - **Truncate**: The packet payload is not saved when it matches the rule, but packet headers and associated meta are retained.
8. In the **Session Options** section, select all options that apply of these four.

- **Assemble:** The assembler assembles the packet chain when it matches the rule.
  - **Network Meta:** The packet generates network metadata when it matches the rule.
  - **Application Meta:** The packet generates application metadata when it matches the rule.
  - **Alert:** The packet generates a custom alert when metadata matches the rule.
9. To save the rule and add it to the rules list, click **OK**.  
The rule is added at the end of the list or inserted where you specified in the context menu.
  10. Check that the rule is in the correct execution sequence with other rules in the list. If necessary, move the rule.
  11. To apply the updated rule set to the Decoder, click **Apply**.  
NetWitness Suite saves a snapshot of the currently applied rules, then applies the updated set to the Decoder and removes the pending indicator from the rules that were pending.

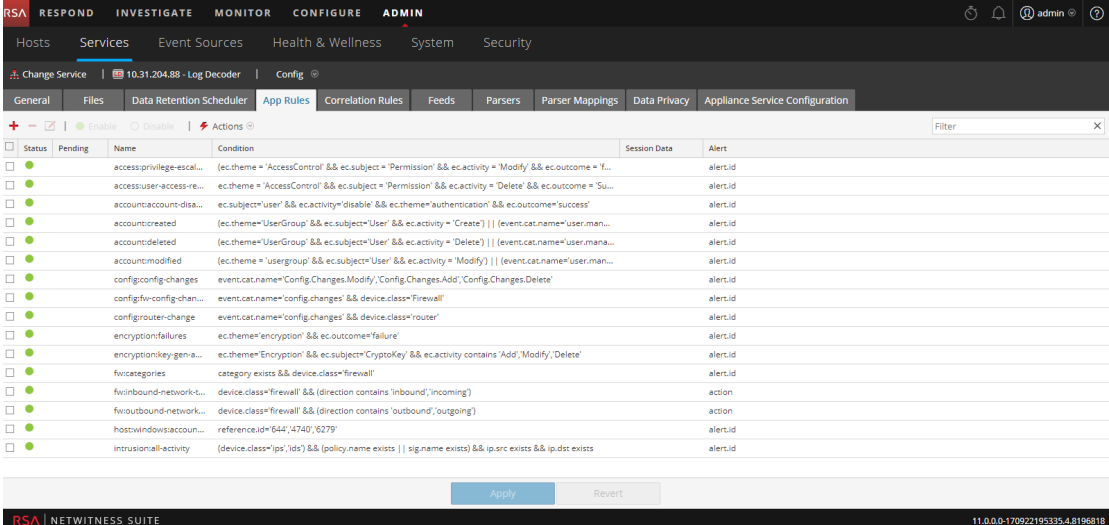
## Fix Rules with Invalid Syntax

After an update to NetWitness Suite 11.0, the user interface highlights any rules with invalid syntax. The Rule Editor provides additional tooltips. After you fix the rules, the highlights disappear. [Configure Decoder Rules](#) provides guidelines that all queries and rule conditions in NetWitness Suite must follow.

### To correct rules with invalid syntax:

1. Go to **ADMIN > Services**.
2. In the **Services** view, select a Decoder and  > **View > Config**.
3. In the **Services Config** view, select one of the Rules tabs: Network Rules, App Rules, or Correlation Rules.

The Rules tab for the selected rule type shows the number of rules using invalid syntax and the invalid rules are highlighted.



Status	Pending	Name	Condition	Session Data	Alert
		accessprivilege-escal...	(ec.theme = 'AccessControl' && ec.subject = 'Permission' && ec.activity = 'Modify' && ec.outcome = 'Y...		alertId
		accessuser-access-re...	ec.theme = 'AccessControl' && ec.subject = 'Permission' && ec.activity = 'Delete' && ec.outcome = 'Su...		alertId
		accountaccount-disa...	ec.subject = 'user' && ec.activity = 'disable' && ec.theme = 'authentication' && ec.outcome = 'success'		alertId
		accountcreated	(ec.theme = 'UserGroup' && ec.subject = 'User' && ec.activity = 'Create')    (event.cat.name = 'user.man...		alertId
		accountdeleted	(ec.theme = 'UserGroup' && ec.subject = 'User' && ec.activity = 'Delete')    (event.cat.name = 'user.man...		alertId
		accountmodified	(ec.theme = 'UserGroup' && ec.subject = 'User' && ec.activity = 'Modify')    (event.cat.name = 'user.man...		alertId
		configconfig-changes	event.cat.name = 'Config.Changes.Modify', 'Config.Changes.Add', 'Config.Changes.Delete'		alertId
		configfw-config-chan...	event.cat.name = 'config.changes' && device.class = 'Firewall'		alertId
		configrouter-change	event.cat.name = 'config.changes' && device.class = 'router'		alertId
		encryptionfailures	ec.theme = 'Encryption' && ec.outcome = 'failure'		alertId
		encryptionkeygen-a...	ec.theme = 'Encryption' && ec.subject = 'CryptoKey' && ec.activity contains 'Add', 'Modify', 'Delete'		alertId
		fwcategories	category exists && device.class = 'firewall'		alertId
		fwinbound-network-t...	device.class = 'firewall' && (direction contains 'inbound', 'incoming')		action
		fwoutbound-network...	device.class = 'firewall' && (direction contains 'outbound', 'outgoing')		action
		hostwindowssaccoun...	reference.id = '644', '4740', '6279'		alertId
		intrusionall-activity	(device.class = 'ips', 'ids') && (policy.name exists    sig.name exists && ip.src exists && ip.dst exists		alertId

4. Select an invalid rule and click .

The Rules Editor shows additional information for the invalid rule and it includes an

additional Save option.

**Rule Editor**

**Rule Definition**

Rule Name: DecTester

Condition: ip.src = "10.30.30.30"

*All string literals and time stamps must be quoted.  
Do not quote number values and ip addresses.  
Examples : 1. device.group='Windows Compliance' && service = 443  
2. time = '2015-jan-01 00:00:00' - u  
3. ip.src = 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16 || extension = 'torrent'*

**Session Data**

☐ Stop Rule Processing

☒ Keep  
☐ Filter  
☐ Truncate

**Session Options**

☒ Alert ☐ Forward ☐ Transient

Alert On: alert.id

This rule is using deprecated rule syntax. To save the changes to this rule independently, correct the syntax and click Save.

Reset Cancel OK Save

5. In the **Condition** field, correct the rule syntax.  
All string literals and time stamps must be quoted. Do not quote number values and IP addresses. [Configure Decoder Rules](#) provides additional details.  
For example, if the invalid rule condition is `ip.src="10.30.30.30"`, correct the syntax by removing the quotes: `ip.src=10.30.30.30`
6. Do one of the following:
  - To correct the rule individually, click **Save**.  
The corrected rule is applied independently to the Decoder. The corrected rule appears on the Rules tab without highlights.
  - To correct the rule and apply the rule to the Decoder later with other rules, click **OK**.  
The corrected rule appears on the Rules tab without highlights. The rule is not applied to the Decoder.

## Decoder Commands for Managing Rules

In the NetWitness Core database, the Rules tree holds the main functionality related to managing rules for all Core services that have rules: Concentrators, Decoders, Log Decoders, and Archivers. Although you can manage rules in the NetWitness Suite user interface, advanced users may prefer to manage rules using a command line to add, merge, replace, delete, and validate rules on a service. This section provides a brief overview of the commands and their usage. These are the available commands:

- `add` - Adds a single rule at the specified position.
- `clear` - Deletes all existing rules in the current node on the service. For example, using the command in `/decoder/config/rules/application` node deletes all existing application rules on the Decoder.
- `delete` - Deletes one or more rules at a specified position and count.
- `merge` - Merges a pushed rule set with an existing rule set. Existing rules that match the incoming rules (by name or rule) are replaced; otherwise, rules are inserted by the position indicated as described in [merge Command](#).
- `replace` - Deletes all existing rules and replaces them with the incoming rule set.
- `validate` - Validates the syntax of a rule, but does not validate the meta keys.

### add Command

The `add` command adds the rule to the existing rule set. Formatting is important because the API uses double quotes in the rule language and also uses double quotes as parameters to all RSA NetWitness® Suite APIs. Therefore, you must escape any double quotes in the rule itself by preceding it with a backslash (`\`) character. This is the syntax of the command:

```
add rule=<string> name=<string> alert=<string, optional> atPos=<<uint32, optional>
```

- `rule` is the rule to add. Be sure to place double quotes around any rules with white space and to escape any double quotes that are part of the rule with a backslash.
- `name` is the name of the rule.
- `alert` is the alert for the rule (if any).
- `atPos` is the position at which the rule should be added (1 based). Zero is the top of the list and any number larger than the current size of the list is appended to the list.

This is an example of command to add a rule using NwConsole

```
send /decoder/config/rules/application add rule="ip.src exists" order=1  
alert=alert.id name=testrule
```

For example, take the following rule:

```
alias.host = "myPC" && country.src="china","russian federation"
```

To add this as a rule, you would need to send the parameters as follows:

```
rule="alias.host = \"myPC\" && country.src=\"china\", \"russian  
federation\"" name=myRule filter
```

Notice how all the double quotes had to be escaped inside the rule parameter. A simple trick to make this more readable is to use single quotes inside the rule. Single and double quotes are interchangeable in the rule and query language, but not in parameters for the API (only double quotes are supported there). Therefore, this is more readable:

```
rule="alias.host = 'myPC' && country.src='china','russian federation'"  
name=myRule filter
```

## merge Command

The `merge` command is used to merge an incoming list of rules with the existing rules on the service. This is how it works:

- It finds existing rules that match via the name OR via a matching rule, updates the existing rule name, and keeps the same position.
- It inserts new rules into the rule list based on the NUMBER position. If the number is zero, it goes to the top of the list.
- It processes the rules in the order received so if you have two rules numbered zero, the second rule is processed after the first and claims the top spot. All existing rules are pushed down two places. Any numbers higher than existing rule positions are appended after the last existing rule and numbered in sequence.
- Any non-numbered rule is appended after the last existing rule and numbered in sequence.

This is the syntax of the merge command:

```
merge --file-data=<string> --file-format<string>
```

- `file-data` is the full path and name of the rules file to merge.
- `file-format` is the format of the rules file. Valid values are `params-list`, `string`, `params`, `binary`, and `params-binary`.



## Methods of Sending a List of Rules to a Service

There are two ways to send a list of rules. You can send them as a `.nwr` (NetWitness Rule) file or as a numbered set of parameters, each number indicates the position to insert the rule at as well as the encoded rule. If you want to see the current list of rules on a service, you need to run the `ls` command on the rule category (for instance, application rules on a Decoder are found in `/decoder/config/rules/application`).

This is an example of commands to list the existing rules using NwConsole:

```
login <hostname>:50004 <username> <password>
cd /decoder/config/rules/application
ls
```

This is another example to list existing rules in NwConsole:

```
send /decoder/config/rules/application ls
```

This is an example of the command to point to network rules in the RESTful port, which supports a basic `admin HTML` app.

```
http[s]://<decoder>:50104/decoder/config/rules/network
```

## Send a NetWitness Rule File

Let's start with an example `nwr` file, each rule must be on a separate line:

```
rule="ip.src=192.168.0.1" name=first keep
rule="ip.src=192.168.1.1" name=second alert=risk.info
rule="ip.src=192.168.2.1" name=third filter
```

To push and merge rules using NwConsole, use the following commands:

```
login <hostname>:50004 <username> <password>
send /decoder/config/rules/application merge --file-data=/root/App_Rules.nwr --file-
format=params-list
```

To replace the existing rules with the rules in the file, instead of using the `merge` command, use the `replace` command.

```
send /decoder/config/rules/application replace --file-data=<pathname> --file-
format=params-list
```

To merge the rules in an `nwr` file using the RESTful port, you can use a `curl` command that pushes the rules:

```
curl -u "<username>:<password>" -H "Content-Type: application/octet-stream" --data-
binary @<pathname> -X POST
"http://<hostname>:50104/decoder/config/rules/application?msg=merge"
```

The examples are pushing application rules. To push network rules, send the rules to `/decoder/config/rules/network`. For correlation rules, send the rules to `/decoder/config/rules/correlation`.

### Send Numbered Parameters

The other way to send a list of rules is to send them as numbered parameters. The difficulty with this method is remembering to escape the quotes within each numbered rule. Though it is only a problem if you are trying to do it by hand. For instance, to send the same rules above as parameters via NwConsole, use the following command:

```
send /decoder/config/rules/application merge 1="rule=\"ip.src=192.168.0.1\"  
name=first keep" 2="rule=\"ip.src=192.168.1.1\" name=second alert=risk.info"  
3="rule=\"ip.src=192.168.2.1\" name=third filter"
```

This command is hard to read because you have to escape the inner quotes with a backslash (`\`). Otherwise, these two commands accomplish the same thing. Merging or adding three rules in positions 1, 2 and 3. If you think the above was hard to read, this is what the equivalent `curl` command looks like:

```
curl -u "<username>:<password>"  
"http://<hostname>:50104/decoder/config/rules/application?msg=merge&1=rule%3D%22ip.src%3D  
192.168.0.1%22%20name%3Dfirst%20keep&2=rule%3D%22ip.src%3D192.168.1.1%22%20name  
%3Dsecond%20alert%3Drisk.info&3=rule%3D%22ip.src%3D192.168.2.1%22%20name%3Dthird  
%20filter"
```

For more details on how to escape double quotes inside parameters, see [add Command](#).

### Ordering Rules When Pushing

Pushed rules are ordered in one of two ways. When passing as parameters, the number of each parameter determines the insertion order. If it is not actually a number, `merge` checks for an `order` parameter within the rule itself and uses that value if found.

**Note:** Using `order` is the only way to set the order with a `.nwr` file. If neither a number nor an `order` parameter is found, there are no guarantees of the insertion order.

### Example

A Decoder has the following application rules installed; notice the numbering is ALWAYS consecutive and starts at 1:

```
0001 : rule="ip.src = 192.168.0.1 || ip.dst = 192.168.0.1 || alias.host = 'My-PC'" name=first keep  
0002 : rule="ip.src=192.168.1.1" name=second alert=risk.info  
0003 : rule="ip.src=192.168.2.1" name=third filter
```

And you want to merge the following four rules:

```
rule="ip.src=192.168.3.1" name=third keep  
rule="ip.dst=192.168.4.1" name=NewRule filter order=0
```

```
rule="alias.host = 'pc1','pc2'" name=filterTheseNames filter order=append
```

```
rule="service=80,443" name=web filter order=3
```

Use any method to push your rules and this is what you end up with:

```
0001 : rule="ip.dst=192.168.4.1" name=NewRule filter order=1
```

```
0002 : rule="ip.src = 192.168.0.1 || ip.dst = 192.168.0.1 || alias.host = 'My-PC'" name=first keep  
order=2
```

```
0003 : rule="service=80,443" name=web filter order=3
```

```
0004 : rule="ip.src=192.168.1.1" name=second alert=risk.info order=4
```

```
0005 : rule="ip.src=192.168.3.1" name=third keep order=5
```

```
0006 : rule="alias.host = 'pc1','pc2'" name=filterTheseNames filter order=6
```

Are there any surprises here? This is how each rule was processed.

1. rule="ip.src=192.168.3.1" name=third keep

This rule had the same name as an existing rule on the Decoder (third). So the rule updated the existing rule, changing `_filter_` to `_keep_`.

2. rule="ip.dst=192.168.4.1" name=NewRule filter order=0

This rule is new and had `order=0` in it, which means insert at the very top.

3. rule="alias.host = 'pc1','pc2'" name=filterTheseNames filter order=append

This rule had a non-number `append` for `order`, therefore, it went to the end of the list. You can accomplish the same thing by giving a very large number, like `999999`.

4. rule="service=80,443" name=web filter order=3

This rule is last but has `order=3`, therefore, if it does not match an existing rule by name or the text of the rule itself, it should be placed in position 3. And there it is, the third rule in the list.

Any rules that follow were pushed further down.

## replace Command

The `replace` command removes all existing rules and replaces them with the incoming rule list. Refer to [merge Command](#) for details on how to format the incoming rule list and how ordering works.

This is an example of the `replace` command using a Netwitness Rule File :

```
send /decoder/config/rules/application replace --file-data=/root/Decoder-AppRules.nwr --file-  
format=string
```

This is an example of the `replace` command using Numbered Parameters :

```
send /decoder/config/rules/application replace 1="rule=\"ip.src exists\" name=\"test rule\" order=1  
alert=alert.id"
```

## clear Command

The `clear` command removes all existing rules on the service. This is an example of the command:

```
send /decoder/config/rules/application clear
```

## delete Command

The `delete` command deletes one or more rules on the service.

`delete atPos <uint32> count <uint32, optional>`

- `atPos` deletes the rule at the given position. Rules are numbered starting with 1 and go in sequential order.
- `count` deletes one or more rules starting `atPos`. This is an optional parameter defining the number of rules to delete starting `atPos`. The default value is 1.

This example of the command deletes four rules beginning at position 0003:

```
send /decoder/config/rules/application delete atPos=0003 count=4
```

## validate Command

The `validate` command takes the provided rule and verifies that it parses correctly. Keep in mind that this command cannot verify whether language keys and entities are valid.

`validate rule <string>`

`rule` - is the name of the rule to validate. Make sure to place double quotes around any rules with white space.

## Configure Feeds and Parsers

---

Feeds and parsers are responsible for analyzing the packets and logs when captured or imported in a Decoder or Log Decoder. Most commonly, they are used for static metadata extraction and service identification. The flexible definition allows custom extension of the core defined services to provide extra service type identification and metadata extraction. This is important due to the volume of custom applications that are used on networks.

**Note:** Unless otherwise stated, any reference to Decoders applies to Log Decoders as well.

### Configure Parsers

NetWitness Suite has a set of core parsers that are defined by the system, and also has the ability to add additional parsers. Each parser is configurable in the [Services Config View - General Tab](#). The Parser Configuration panel provides a way to enable or disable parsers to use on the Decoder in addition to limiting the metadata that the parser creates.

In addition, there are several types of custom configurable parsers:

- GeoIP – This parser associates the IP addresses with geographical locations.
- Search – This parser is user -configured to generate metadata by scanning for pre -defined keywords and regular expressions.
- FLEXPARSE (deprecated) – This is a generic parser definition language for extending the existing application protocol support of the Decoder. By default this parser is disabled (see [Enable or Disable Lua and Flex Parsing Systems](#)).
- Lua – This parser is defined using the Lua scripting language for extending the existing application protocol support of the Decoder.
- enVision – This application parser supports the Log Decoder and is configured to generate metadata by scanning log files.
- SNORT® – This parser supports the payload detection capabilities of SNORT® IDS rules.

In the Services Config view > Parsers tab, you can view deployed parsers on a Decoder, upload parsers, and delete deployed parsers. The user interface includes an Indicator if the parser originated from Live Services, installed through NetWitness Suite, or uploaded manually. Parsers can be added and removed while a Decoder is running without affecting capture.

In addition, you can download parsers using NetWitness Suite Live Services.

## Configure Feeds

NetWitness Suite uses feeds to create metadata based on externally defined metadata values. A feed is a list of data that is compared to sessions as they are captured or processed. For each match, additional metadata is created. This data could identify and classify malicious IPs or incorporate additional information such as department and location based on internal network assignments. Some examples of feeds include threat feeds to identify BOTNets, DHCP mappings, or even active directory information such as physical location or logical department.

You can use the Live module in NetWitness Suite to obtain feeds from outside sources. "Live Content in NetWitness Suite" in the *Live Services Management Guide* provides an overview of the Live content management tool.

Within the NetWitness Suite user interface, you can view the list of currently deployed feeds, along with an indicator if a feed that originated from Live was installed through NetWitness Suite or manually. Feeds can be added, removed, and updated while a Decoder is running without affecting capture.

has a Custom Feed wizard to allow creation and deployment of custom Decoder feeds based on deterministic logic that offers the meta keys specific to the selected Decoders and Log Decoders. Although the wizard guides users through the process to create both on-demand and recurring feeds, it is helpful to understand the form and content of a feed file when you create a feed.

NetWitness Suite has a Custom Feed wizard, which streamlines the task of creating and managing custom feeds, as well as populating the feeds to selected Decoders and Log Decoders. In addition, you can download existing feed files and edit the files, then edit the feed or create a new feed using the edited file.

## Custom Feed Definition File Structure

The NetWitness Suite Custom Feed wizard allows creation and deployment of custom Decoder feeds based on deterministic logic that offers the meta keys specific to the selected Decoders and Log Decoders. Although the wizard guides users through the process to create both on-demand and recurring feeds, it is helpful to understand the form and content of a feed file when you create a feed.

Feed filenames 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 format and a feed definition file in .xml format, which describes the structure of a feed data file. The 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 Custom Feed wizard. 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" />
      </LanguageKeys>
    </FlatFileFeed>
  </FDF>
```

```

        <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 Custom Feed wizard provides 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: <b>Default</b> - to define a feed based on a .csv formatted feed data file. <b>STIX</b> - to define a feed based on STIX formatted.xml file.
(Define Feed Tab) Feed Task Type	Select: <b>Adhoc</b> - to create an on-demand feed. <b>Recurring</b> - to update the .csv or .xml file persistently and store it in a location accessible by NetWitness Suite , so NetWitness Suite downloads a file at regular intervals and pushes it to the downstream devices.
(Define Feed tab) <b>Name</b>	The custom feed name in the feed data file. It corresponds to the <code>flatfeedfile name</code> attribute in the feed definition file. For example, Dynamic DNS Test Feed. <div> <b>Note:</b> You can use special characters to define the name of the custom feed.           </div>



NetWitness Suite Parameter	Feed Definition File Equivalent
(Define Feed tab) <b>File/Browse</b>	This is the name of the feed data file. It corresponds to the <code>flatfeedfile path</code> attribute in the feed definition file. For example, <code>dynamic_dns.csv</code> .
(Advanced Options tab) <b>XML Feed File</b>	The name of the feed definition file. For example, <code>dynamic_dns.xml</code> .
(Advanced Options tab) <b>Separator</b>	The separator character used to separate attributes in the feed data file. It corresponds to the <code>latfeedfile separator</code> in the feed definition file. For example, a comma.
(Advanced Options tab) <b>Comment</b>	The character used to identify a comment in the feed data file. It corresponds to the <code>flatfeedfile comment</code> attribute in the feed definition file. For example, <code>#</code> .
(Define Columns tab, Define Index) <b>Type</b>	<p>The type of lookup value in the index position of the feed data file.</p> <p><b>IP</b> means that each row in the feed data file contains an IP address in the lookup value position. The IP value is in dotted-decimal format (for example, <code>10.5.187.42</code>).</p> <p><b>IP Range</b> means that each row in the feed data file contains a range of IP addresses in the lookup value position. The IP range is in CIDR format (for example, <code>192.168.2.0/24</code>).</p> <p><b>Non IP</b> means that the each row in the feed data file contains a metadata value other than IP address in the lookup value position. The Service Type and Truncate Domain, and Callback Keys fields become active for a Non IP index.</p>

NetWitness Suite Parameter	Feed Definition File Equivalent
(Define Columns tab, Define Index) <b>CIDR</b>	Specifies that the IP value in the lookup position is in CIDR format. The <b>CIDR</b> attribute sets the IP address format in the field to Classless Inter-Domain Routing (CIDR) notation.
(Define Columns tab, Define Index) <b>Service Type</b>	For a Non IP index, the integer service type to filter meta lookups. It corresponds to the <code>MetaCallback apptype</code> attribute in the feed definition file. A value of 0 indicates no filtering by service type.
(Define Columns tab, Define Index) <b>Truncate Domain</b>	For a Non IP index, for meta values that contain domain names (for example, hostnames), the system can strip off the host specific element in the data. Truncate Domain corresponds to the <code>MetaCallback truncdomain</code> attribute. If the value is <code>www.example.com</code> , it is truncated to <code>example.com</code> . A value of <b>False</b> selects no truncation, and <b>True</b> selects truncation.
(Define Columns tab, Define Index) <b>Callback Keys</b>	For a Non IP index, the available meta keys to match on instead of <code>ip.src/ip.dst</code> (the defaults for IP index type) are selectable from the drop-down list. The Callback Key corresponds to the <code>MetaCallback name</code> 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) <b>Index Column</b>	Identifies the column in the feed data file that provides the lookup value for the row. Each position in each row of the feed data file is identified by a <b>Field index</b> attribute in the feed definition file. A field with an index of <b>1</b> is the first entry in a row, the second field has an index of <b>2</b> , the third field has an index of <b>3</b> , and so on.

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

## Sample Files for a MetaCallback Feed Using CIDR Index Range for IPv4 and IPv6

These sample files demonstrate 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>
  </FlatFileFeed>
  <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 Custom Feed

You can 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.

**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.

The feed data file 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 **CONFIGURE > Custom Feeds**, and in the **Feeds** panel click **+**.  
The Custom Feeds view is displayed.

The screenshot shows the NetWitness Suite interface with the 'CUSTOM FEEDS' tab selected. The 'Feeds' panel is active, displaying a table of configured feeds. The table has the following data:

Name	Trigger	Disk Usage	Created	Last Run Time	Status	Progress
TEST	Once	-	2017-07-13 13:30:36	2017-07-13 13:30:36	Completed	<div style="width: 100%;"></div>
TEST2	Once	-	2017-07-13 13:50:33	2017-07-13 13:50:33	Completed	<div style="width: 100%;"></div>
te	Once	-	2017-07-14 04:16:51	2017-07-14 04:16:51	Completed	<div style="width: 100%;"></div>
onlydom	Once	-	2017-07-14 04:21:37	2017-07-14 04:21:37	Completed	<div style="width: 100%;"></div>
PCAP	Once	-	2017-07-14 09:30:49	2017-07-14 09:30:49	Completed	<div style="width: 100%;"></div>

2. Click **Custom Feed** and **Next**.

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

The screenshot shows a wizard window titled "Configure a Custom Feed" with a close button (X) in the top right corner. The wizard has four steps: "Define Feed" (active), "Select Services", "Define Columns", and "Review".

Under "Define Feed", there are two sections:

- Feed Type:** Two radio buttons, "CSV" (selected) and "STIX".
- Feed Task Type:** Two radio buttons, "Adhoc" (selected) and "Recurring".

Below these are two required fields:

- Name \***: A text input field.
- File \***: A text input field with the placeholder "Select File" and a "Browse" button to its right.

At the bottom of the form is a section for "Advanced Options" with a dropdown arrow and the text "Advanced Options".

At the bottom of the wizard are four buttons: "Reset", "Cancel", "Prev", and "Next" (highlighted in blue).

3. Select the Feed Type: **CSV** or **STIX**.
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:

The screenshot shows a dialog box titled "Configure a Custom Feed" with a close button (X) in the top right corner. The dialog has four tabs: "Define Feed" (active), "Select Services", "Define Columns", and "Review".

Under the "Define Feed" tab, there are two radio buttons for "Feed Task Type": "Adhoc" (selected) and "Recurring". Below these are two text input fields: "Name \*" containing "Test" and "File \*" containing "testprange.csv". To the right of the "File \*" field is a "Browse" button.

Below the input fields is a section titled "Advanced Options" with a downward arrow icon. The area below this section is empty.

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

- 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.



Configure a Custom Feed

Define Feed
















Select Services

Define Columns

Review

Services

Groups

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

Reset

Cancel

Prev

Next

- 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.

The screenshot shows the 'Configure a Custom Feed' dialog box with the 'Define Feed' tab selected. The dialog has four tabs: 'Define Feed', 'Select Services', 'Define Columns', and 'Review'. In the 'Define Feed' tab, the 'Feed Task Type' is set to 'Recurring' (radio button selected). Below this are fields for 'Name \*' and 'URL \*'. The 'URL \*' field has a 'Verify' button next to it. There are checkboxes for 'Authenticated' and 'Use proxy', both of which are currently unchecked. Below these is a 'Recur Every' field with a spinner and a dropdown menu. A 'Date Range' section is collapsed. An 'Advanced Options' section is expanded, showing fields for 'XML Feed File' (with a 'Select File' button and a 'Browse' button), 'Separator' (with a dropdown showing a comma), and 'Comment' (with a dropdown showing a hash symbol). At the bottom of the dialog are buttons for 'Reset', 'Cancel', 'Prev', and 'Next'.

- 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 verifies the location where the file is stored in order to enable checking 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 server to access the Feed URL through a proxy, select **Use Proxy**. For more information on configuring a proxy, see "Configure Proxy for NetWitness Suite" 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.

The screenshot shows the 'Configure a Custom Feed' dialog box with the 'Define Feed' tab selected. The dialog has four tabs: 'Define Feed', 'Select Services', 'Define Columns', and 'Review'. The 'Feed Task Type' is set to 'Recurring'. The 'Name' field contains 'TestFeed'. The 'URL' field contains 'https://qasa2.netwitness.local/live/feeds'. There are checkboxes for 'Authenticated' and 'Use proxy', both of which are unchecked. The 'Recur Every' field is set to '3' and the unit is 'Day(s)'. There is a 'Date Range' section with a dropdown arrow. The 'Advanced Options' section is expanded, showing 'XML Feed File' with a 'Select File' button and a 'Browse' button. The 'Separator' field contains a comma (',') and the 'Comment' field contains a hash symbol ('#'). At the bottom of the dialog are buttons for 'Reset', 'Cancel', 'Prev', and 'Next'.

**Configure a Custom Feed**

**Define Feed** | Select Services | Define Columns | Review

Feed Task Type: ☐ Adhoc ☒ Recurring

Name \*:

URL \*:

☐ Authenticated

☐ Use proxy

Recur Every:

—

XML Feed File:

Separator:

Comment:

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.

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

Reset Cancel Prev Next

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

The Define Columns form is displayed.

- 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.

**Configure a Custom Feed**

Define Feed | Select Services | **Define Columns** | Review

**Define Index**

Type: ☐ IP ☐ IP Range ☒ Non IP

Index Column: 1 Service Type: 0 ☒ Truncate Domain

Callback Key (S):

**Define Values**

Column	Key
1 (Index)	
SRM_Sa	
ANCEST	

OS  
access.point  
accesses  
action  
alert  
alert.id  
alias.host  
alias.ip  
alias.ipv6  
alias.mac  
asn.dst  
asn.src

Reset Cancel Prev Next

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

Configure a Custom Feed

Define Feed

Select Services

Define Columns

Review

Define Index

Type

☐ IP

☐ IP Range

☒ Non IP

Index Column

1

Service Type

0

☒ Truncate Domain

Callback Key (S)

action

Define Values

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

Reset

Cancel

Prev

Next

- e. Click **Next**.

The Review form is displayed.

**Configure a Custom Feed**

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

**Feed Details**

Name: Testing  
CSV File: AssetsImportCompleteSample.csv

**Service Details**

Services: Log Decoder, Decoder

**Column Mapping Details**

Index Type: Other  
Callback Key(s): action  
Truncate Domain: true  
Service Type: 0  
Value Columns:

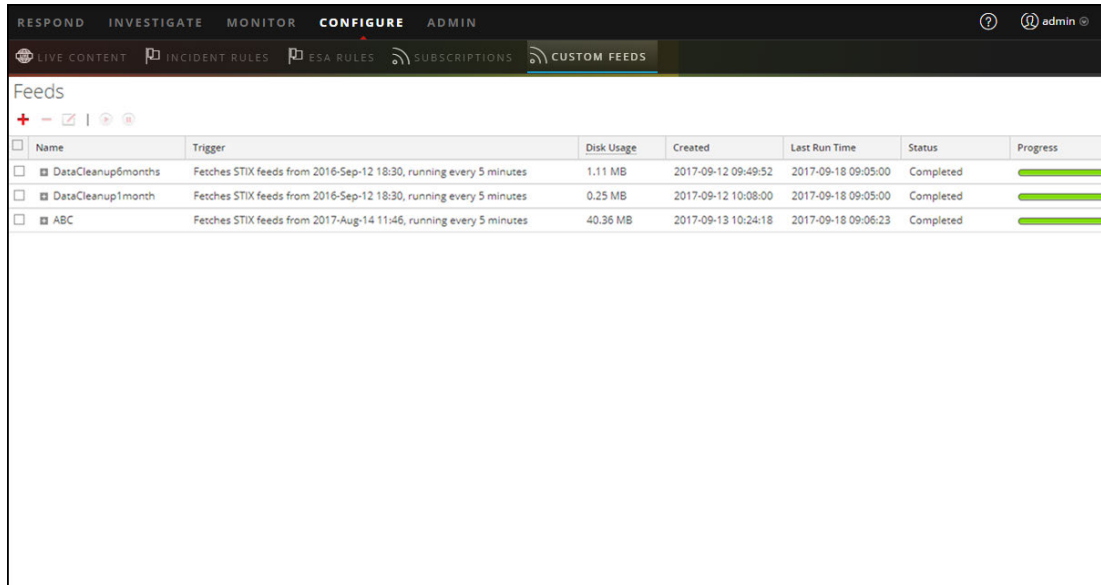
1	2	3	4
Index	threat.source	threat.category	threat.desc

Reset Cancel Prev **Finish**

10. Anytime before you click **Finish**, you can:
  - Click **Cancel** to close the wizard without saving your feed definition.
  - Click **Reset** to clear the data in the wizard.
  - Click **Next** to display the next 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.

..



<input type="checkbox"/>	Name	Trigger	Disk Usage	Created	Last Run Time	Status	Progress
<input type="checkbox"/>	DataCleanup6months	Fetches STIX feeds from 2016-Sep-12 18:30, running every 5 minutes	1.11 MB	2017-09-12 09:49:52	2017-09-18 09:05:00	Completed	<div></div>
<input type="checkbox"/>	DataCleanup1month	Fetches STIX feeds from 2016-Sep-12 18:30, running every 5 minutes	0.25 MB	2017-09-12 10:08:00	2017-09-18 09:05:00	Completed	<div></div>
<input type="checkbox"/>	ABC	Fetches STIX feeds from 2017-Aug-14 11:46, running every 5 minutes	40.36 MB	2017-09-13 10:24:18	2017-09-18 09:06:23	Completed	<div></div>



## Create a STIX Custom Feed

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/>.

You can create a custom feed using a STIX-formatted feed data file (.xml) in RSA NetWitness Suite. NetWitness Suite supports Structured Threat Information Expression (STIX) 1.0, 1.1 and 1.2 versions only.

**Caution:** If a 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 feeds of type Indicator or Observable that contain properties such as the IP addresses, File hashes, Domain names, URIs and Email addresses are supported. The properties values in the Equals operator are supported. Attributes such as Type and Title are also read from the STIX. A STIX file with a single STIX\_Package is 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.

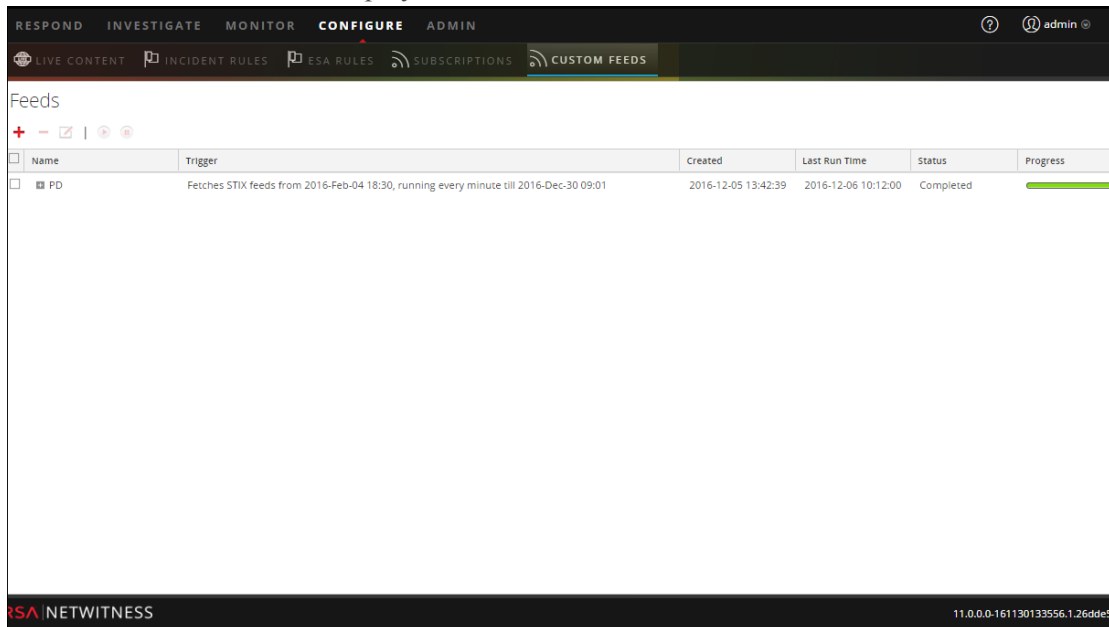
Apart from the TAXII server, STIX data can also reside on a REST server and you can fetch the STIX file from the REST server by providing the URL of the REST server. For example, `http://stixrestserver.internal.com`.

The STIX feed data file and optionally the feed definition file, both in .xml format 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:

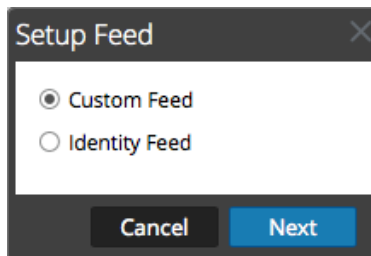
1. Go to **Configure > Custom Feeds**.

The 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 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), specify the **Comment** characters used in the feed data file (default is #), and click **Next**.

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

**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**.

<input type="checkbox"/>		Name ^	Address	Type
<input type="checkbox"/>		STIX Content Hub	10.10.10.10	Log Decoder
<input checked="" type="checkbox"/>		STIX Content Hub	10.10.10.10	Context Hub
<input type="checkbox"/>		STIX Content Hub	10.10.10.10	Log Decoder
<input type="checkbox"/>		STIX Content Hub	10.10.10.10	Decoder

Reset Cancel Prev **Next**

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.

The screenshot shows the 'Configure a Custom Feed' dialog box with the 'Define Feed' tab selected. The dialog has four tabs: 'Define Feed', 'Select Services', 'Define Columns', and 'Review'. The 'Define Feed' tab contains the following fields and options:

- Feed Type:** Radio buttons for CSV and STIX (selected).
- Feed Task Type:** Radio buttons for Adhoc and Recurring (selected).
- Name \*:** Text field containing 'Test Feed1'.
- URL \*:** Text field containing 'http://stixrestserver.internal.com' with a 'Verify' button to its right.
- Authentication Options:**
  - ☐ Authenticated
  - ☐ Use proxy
  - ☐ TAXII Enabled Server
- Recur Every:** A numeric spinner set to '1' and a dropdown menu set to 'Hour(s)'.
- ☐ Date Range
- Advanced Options:** A section header with a checkmark icon.

At the bottom of the dialog are four buttons: 'Reset', 'Cancel', 'Prev', and 'Next'.

- 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:** A 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 the 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 and 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 "Configure Proxy for NetWitness Suite" in the *System Configuration Guide*. (Go to the [Master Table of](#)

[Contents](#) for Version 11.0 to find NetWitness Suite 11.0 documents.) 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 as Authentication, Proxy, Certificate trust, TAXII Enabled Server, and others, are configured before you click Verify.

- i. To define the interval of recurrence for pushing to the 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.
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**.

<input type="checkbox"/>	Name ^	Address	Type
<input type="checkbox"/>	STIX Content Hub	STIX Content Hub	Log Decoder
<input checked="" type="checkbox"/>	STIX Content Hub	STIX Content Hub	Context Hub
<input type="checkbox"/>	STIX Content Hub	STIX Content Hub	Log Decoder
<input type="checkbox"/>	STIX Content Hub	STIX Content Hub	Decoder

Reset Cancel Prev **Next**

If the data from the STIX server is large, the following message is displayed:  
 "Fetching sample data is taking longer than expected. Choose one of the following options." You have two options: continue to wait or map without sample data.

- If you click **Continue to Wait**, the Feed Wizard continues to wait till the sample data is fetched or a timeout (10 minutes) occurs, whichever is sooner. If there is a timeout, no sample data is retrieved.
- 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.



Configure a Custom Feed

Define Feed Select Services **Define Columns** Review

Define Index

Type ☒ IP ☐ Non IP

Index Column  ☐ CIDR

Define Values

Column	1	2	3	4
Key	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	Indicator Title	Indicator Description	Observable Title	Observable Description
	This domain p57A5E9...	torstatus.blutmagie.de...	IP: 87.145.233.207	IPv4: 87.145.233.207  ...
	This domain p57A5E9...	torstatus.blutmagie.de...	Domain: p57A5E9CF.d...	Domain: p57A5E9CF.d...

Reset Cancel Prev **Next**

- If the Index Type is Non IP, you can select multiple index columns in the Index Columns. 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 Columns 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 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.

**Configure a Custom Feed**

Define Feed | Select Services | Define Columns | **Review**

**Feed Details**

Name	Both2		
URL	http://10.31.204.238/taxii-discovery-service		
TAXII Collection	admin.blacklisted.ip		
Recurrence Type	Every 1 Minute (s)		
Date Range	Start Date	End Date	
	2016-03-05T00:00:00	2016-12-05T13:45:55	

**Service Details**

Services	CH-241, Packet Decoder - Decoder, LD - Log Decoder
----------	----------------------------------------------------

**Column Mapping Details**

Index Type	IP
CIDR	false
Value Columns	

1  
ind.title

2  
ind.desc

3  
obs.title

4  
obs.desc

5  
Index

Reset
Cancel
Prev
Finish

10. Anytime before you click **Finish**, you can:
  - Click **Cancel** to close the wizard without saving your feed definition.
  - Click **Reset** to clear the data in the wizard.
  - Click **Next** to display the next 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, 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.

RESPOND INVESTIGATE MONITOR <b>CONFIGURE</b> ADMIN							
LIVE CONTENT INCIDENT RULES ESA RULES SUBSCRIPTIONS <b>CUSTOM FEEDS</b>							
Feeds							
+ -							
<input type="checkbox"/>	Name	Trigger	Disk Usage	Created	Last Run Time	Status	Progress
<input type="checkbox"/>	DataCleanup6months	Fetches STIX feeds from 2016-Sep-12 18:30, running every 5 minutes	1.11 MB	2017-09-12 09:49:52	2017-09-18 09:05:00	Completed	<div></div>
<input type="checkbox"/>	DataCleanup1month	Fetches STIX feeds from 2016-Sep-12 18:30, running every 5 minutes	0.25 MB	2017-09-12 10:08:00	2017-09-18 09:05:00	Completed	<div></div>
<input type="checkbox"/>	ABC	Fetches STIX feeds from 2017-Aug-14 11:46, running every 5 minutes	40.36 MB	2017-09-13 10:24:18	2017-09-18 09:06:23	Completed	<div></div>


**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*.

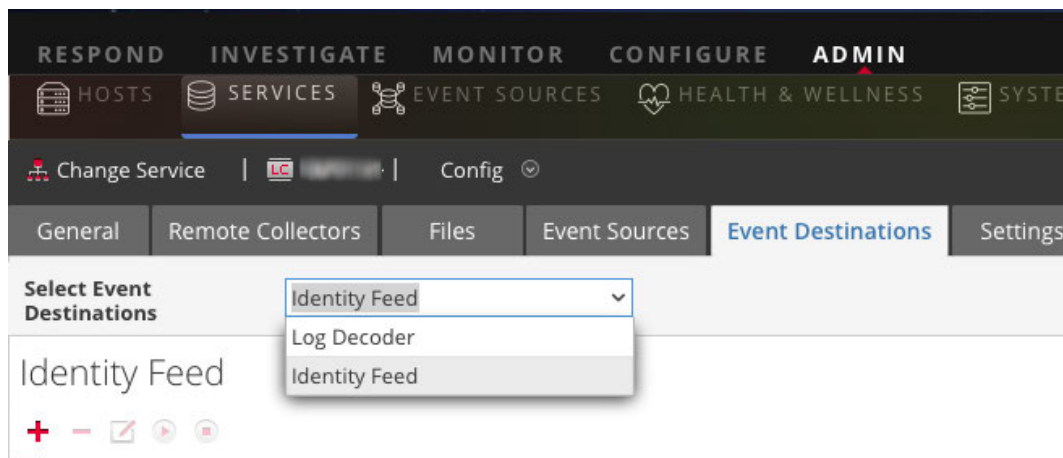
## Create an Identity Feed

You can create an Identity feed and populate it to selected Decoders and Log Decoders. In order to create an identity feed, you need to have:

- A Log Collector service with an Identity Feed Event Processor
- A Log Collector service with Windows Collection configured and enabled

### 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.

**Add Identity Feed**

Name \*

Queue

Rollover Interval

Update Interval

Event Source Filter

Start Processor On Service Startup ☒

Cancel OK

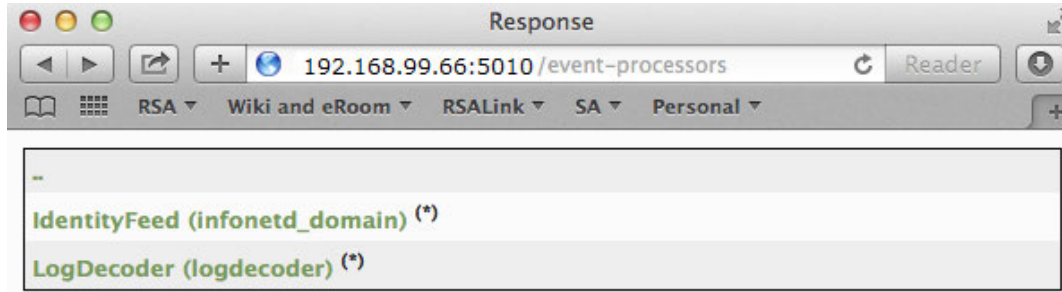
- e. Click **OK**.
2. Test generation of messages.
  - a. Have users log into Windows boxes on the domain to generate the appropriate log messages on the domain controllers for testing.
  - b. Verify that data is written to the feed files. SSH to the Log Decoder/Collector or Virtual Log Collector being configured. Navigate to `/var/netwitness/logcollector/runtime/identity-feed` and verify that the `Identity_deploy` files are getting populated with data.

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

- c. Open up a web browser (Non-Internet 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**

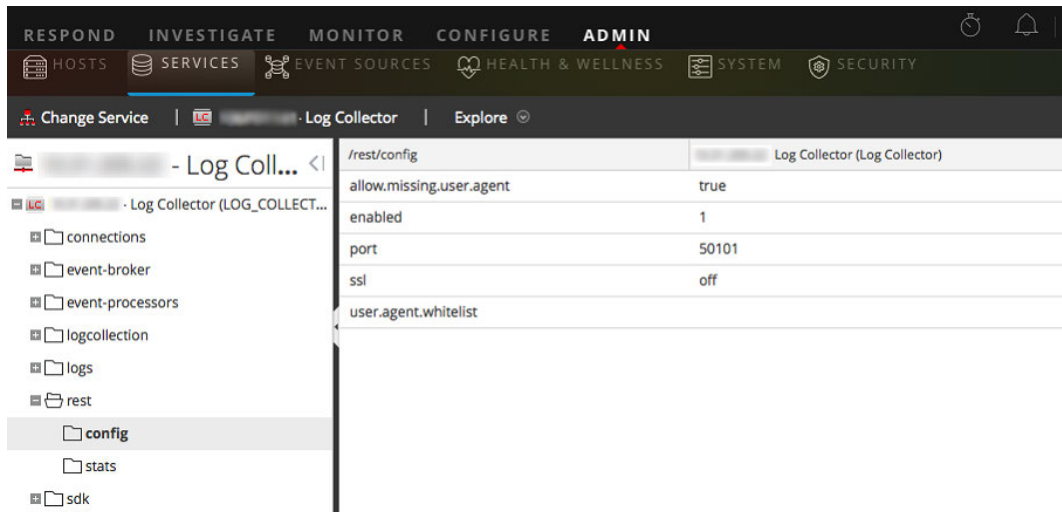
The browser screen should look like this:



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.

- Go to **AdMIN > Services > <Log Collector being setup>** **> View > Explore**.
- In the left pane, expand **rest > config**.



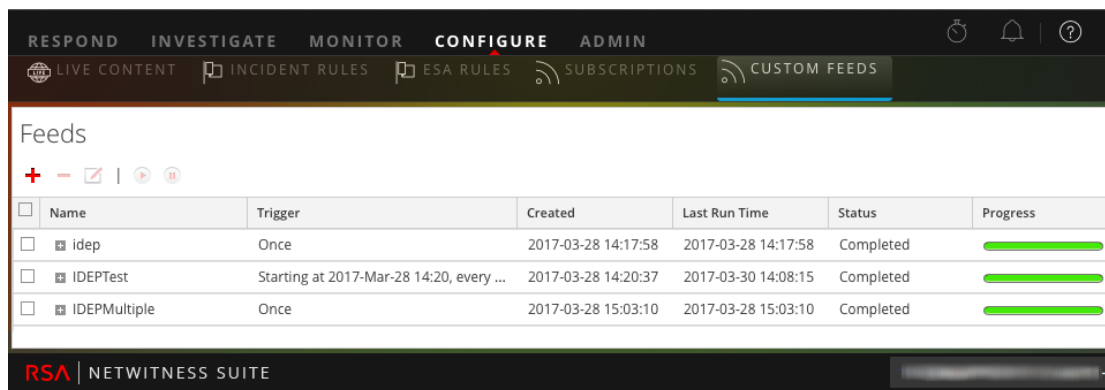
For REST to be active, **enabled** must be set to **1**.

- 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.

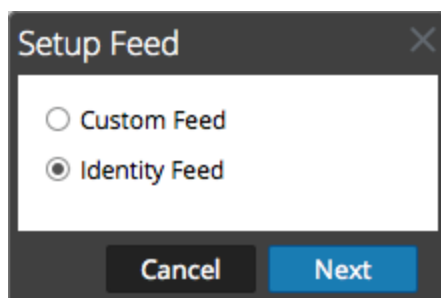
- Go to **CONFIGURE > Live Content > Custom Feeds**.

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 Version 11.0 to find NetWitness Suite 11.0 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.

The screenshot shows a 'Configure Identity Feed' dialog box with three tabs: 'Define Feed', 'Select Services', and 'Review'. The 'Select Services' tab is active. It contains two sub-tabs: 'Services' (selected) and 'Groups'. Below the sub-tabs is a table with columns: 'Name ^', 'Address', and 'Type'. There are two rows of data, each with a checkbox and a green leaf icon to its left. The first row is 'Decoder' and the second is 'Log Decoder'. At the bottom of the dialog are four buttons: 'Reset', 'Cancel', 'Prev', and 'Next'.

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

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.

**Configure Identity Feed**

Define Feed | **Select Services** | Review

[Feed Details](#)

Name	Testing
Feed File	zip sample.zip

[Service Details](#)

Services	Decoder
----------	---------

Reset Cancel Prev **Finish**

**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.

RESPOND INVESTIGATE MONITOR <b>CONFIGURE</b> ADMIN							
LIVE CONTENT INCIDENT RULES ESA RULES SUBSCRIPTIONS <b>CUSTOM FEEDS</b>							
Feeds							
+ - [ ] [ ] [ ] [ ]							
<input type="checkbox"/>	Name	Trigger	Disk Usage	Created	Last Run Time	Status	Progress
<input type="checkbox"/>	DataCleanup6months	Fetches STIX feeds from 2016-Sep-12 18:30, running every 5 minutes	1.11 MB	2017-09-12 09:49:52	2017-09-18 09:05:00	Completed	<div></div>
<input type="checkbox"/>	DataCleanup1month	Fetches STIX feeds from 2016-Sep-12 18:30, running every 5 minutes	0.25 MB	2017-09-12 10:08:00	2017-09-18 09:05:00	Completed	<div></div>
<input type="checkbox"/>	ABC	Fetches STIX feeds from 2017-Aug-14 11:46, running every 5 minutes	40.36 MB	2017-09-13 10:24:18	2017-09-18 09:06:23	Completed	<div></div>

## Import the SSL Certificate

If SSL is configured on the Identity feed's Log Collector, follow these steps to import the Log Collector's SSL certificate into the 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 **jetty** to allow jetty to read the new certificate in the store.

## Cannot Verify Identity Feed URL

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

If there are 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.

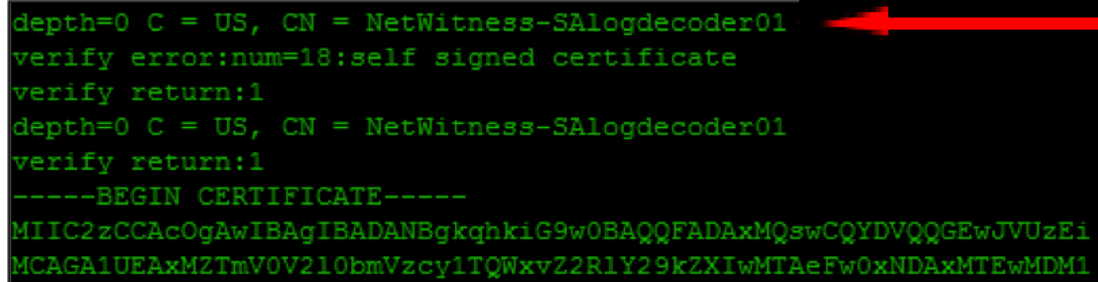
1. SSH to the Security Analytics UI server.
2. Run the following command to output the CN name of the SSL cert:

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

Example:

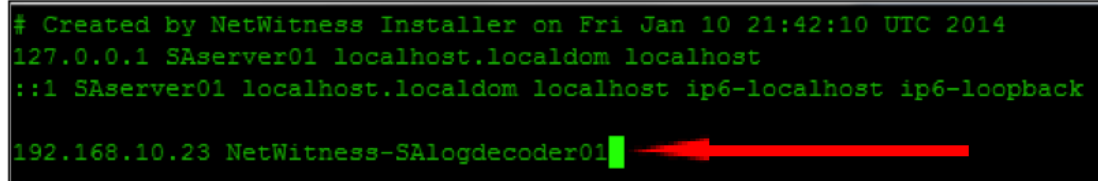
```
echo -n | openssl s_client -connect salogdecoder01:50101 |
sed -ne '/BEGIN CERTIFICATE-/, /-END CERTIFICATE-/p'
```

3. Retrieve the CN name of the SSL certificate.



```
depth=0 C = US, CN = NetWitness-SALogdecoder01
verify error:num=18:self signed certificate
verify return:1
depth=0 C = US, CN = NetWitness-SALogdecoder01
verify return:1
-----BEGIN CERTIFICATE-----
MIIC2zCCAcOgAwIBAgIBADANBgkqhkiG9w0BAQQFADAxMQswCQYDVQQGEwJVUzEi
MCAGA1UEAxMZTmV0V210bmVzcy1TQWxvZ2R1Y29kZXIwMTAeFw0xNDExMTEwMDM1
```

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



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

5. Restart the network service on the appliance.

6. Confirm that the name placed in the **/etc/hosts** file is used instead of the FQDN or IP address in the Identity feed URL.
7. Re-verify the Identity feed URL.

## Edit, Upload, or Remove a Feed

You can upload a feed, edit an existing feed, or remove a feed.

### To edit an existing feed:

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

The Feeds view is displayed.

Name	Trigger	Disk Usage	Created	Last Run Time	Status	Progress
TEST	Once	-	2017-07-13 13:30:36	2017-07-13 13:30:36	Completed	<div></div>
TEST2	Once	-	2017-07-13 13:50:33	2017-07-13 13:50:33	Completed	<div></div>
te	Once	-	2017-07-14 04:16:51	2017-07-14 04:16:51	Completed	<div></div>
onlydom	Once	-	2017-07-14 04:21:37	2017-07-14 04:21:37	Completed	<div></div>
PCAP	Once	-	2017-07-14 09:30:49	2017-07-14 09:30:49	Completed	<div></div>
myCSV	Once	-	2017-07-18 22:20:12	2017-07-18 22:24:06	Completed	<div></div>

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

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



The screenshot shows a 'Configure a Custom Feed' dialog box with a dark header and a light gray body. The header has a close button (X) in the top right corner. Below the header is a progress bar with four steps: 'Define Feed' (active, dark gray), 'Select Services' (light gray), 'Define Columns' (light gray), and 'Review' (light gray). The 'Define Feed' section contains the following fields and options:

- Feed Type:** Two radio buttons, 'CSV' (unselected) and 'STIX' (selected).
- Feed Task Type:** Two radio buttons, 'Adhoc' (selected) and 'Recurring' (unselected).
- Name \*:** A text input field containing 'TEST'.
- File \*:** A text input field containing 'TEST-stix.xml'. To the right of this field is a 'Browse' button. Below the field is a blue link labeled 'download file'.
- Advanced Options:** A section header with a downward arrow icon.

At the bottom of the dialog box is a dark gray bar with four buttons: 'Reset' (dark gray), 'Cancel' (dark gray), 'Prev' (light gray), and 'Next' (blue).

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. For a STIX feed, the .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 recreated with the updated file and new feed specifications. 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.

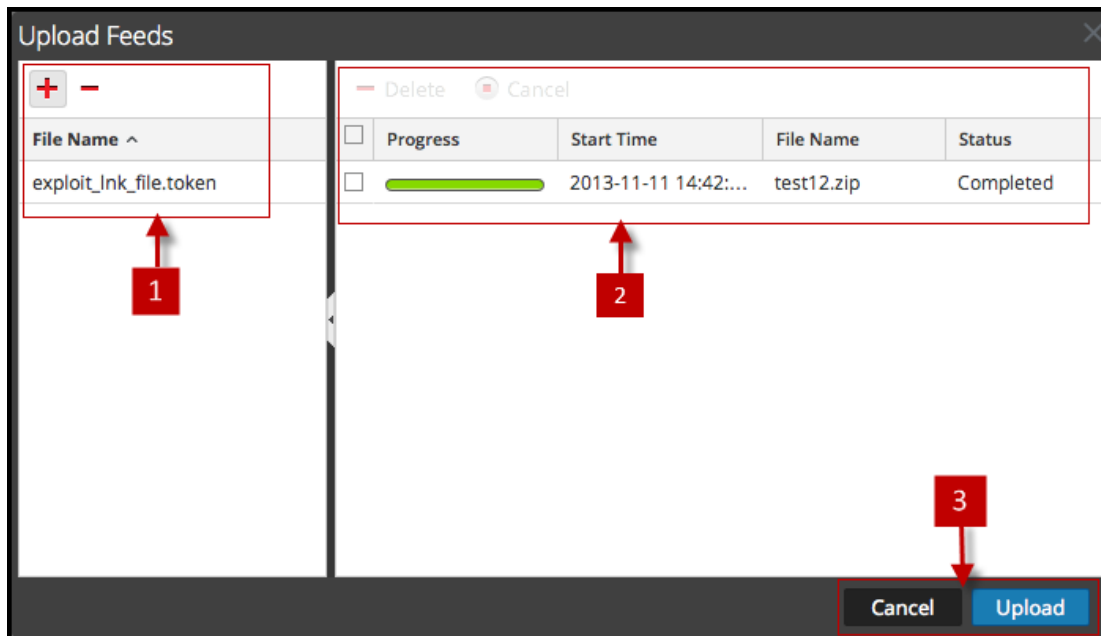
### To upload a feed to a Dcoder or Log Decoder:

1. Go to **ADMIN > Services**.
2. Select a service and click  > **View > Config**.

The Services Config view is displayed with the General tab open.

3. Select the **Feeds** tab.
4. In the Feeds tab toolbar, click  **Upload**.

The Upload Feeds dialog is displayed.



5. In the **File** grid, click **+** and select a feed file. Supported files are \*.feed, \*.token, and \*.filter.

6. Select the feed file from the **File** list and click **Upload**.

The Upload Job list is updated to show the progress and status of the uploaded feed.

#### To remove a feed:

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

The Custom Feeds view is displayed.

Name	Trigger	Disk Usage	Created	Last Run Time	Status	Progress
TEST	Once	-	2017-07-13 13:30:36	2017-07-13 13:30:36	Completed	100%
TEST2	Once	-	2017-07-13 13:50:33	2017-07-13 13:50:33	Completed	100%
te	Once	-	2017-07-14 04:16:51	2017-07-14 04:16:51	Completed	100%
onlydom	Once	-	2017-07-14 04:21:37	2017-07-14 04:21:37	Completed	100%
PCAP	Once	-	2017-07-14 09:30:49	2017-07-14 09:30:49	Completed	100%
myCSV	Once	-	2017-07-18 22:20:12	2017-07-18 22:24:06	Completed	100%

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

The Delete Custom Feeds dialog is displayed.

**Delete Custom Feeds**

☐ Local DB and Service  
☒ Local DB Only  
☐ Service Only

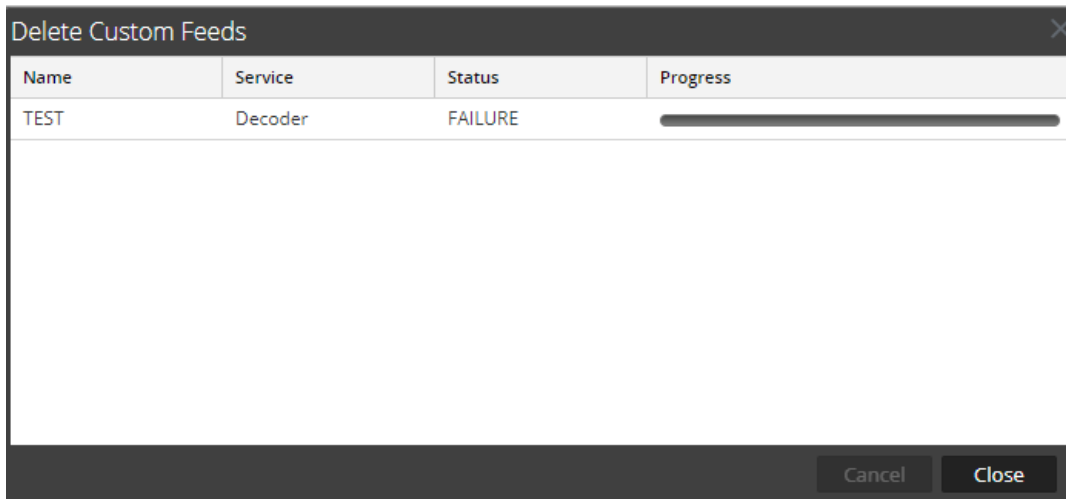
Cancel Delete

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 be 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.

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.



## Create Custom Meta Keys Using a Custom Feed

This topic provides information on how to add custom meta keys, using a custom feed in the Log Decoder.



You can create custom meta keys to retrieve data, to investigate and analyze the logs and packets. Custom meta keys enable you to add an enrichment context for the log and packet data. This document highlights the configuration changes to reflect the custom meta keys in the Concentrator, ESA, Archiver, Warehouse Connector, and Reporting Engine schema.

Here is an example of creating the custom meta key in the Log Decoder. In this scenario, an organization wants to track the location of an asset such as a printer. So, a custom meta key **source location** is introduced, which indicates the location of the asset, for example Printer1, which is located in the 'Fifth Floor A wing'.

**Note:** Custom meta keys can be created in the Decoder as well. Select the `index-decoder-custom.xml` file when you create a custom meta in the Decoder.

### Add a Custom Meta Key in the Log Decoder

To add custom meta keys using custom feed:

1. Go to **ADMIN > Services > Log Decoder**.
2. Select a service and click   > **View > Config > Files tab > index-logdecoder-custom.xml**.

```
<Language>
  <?xml version="1.0" encoding="utf-8"?>
  <Language level="IndexNone" defaultAction="Auto">
    <!-- Reserved Meta key for Feed -->
    <Key description="Source Location" level="IndexNone"
      name="location.src" format="Text"/>
  </Language>
```

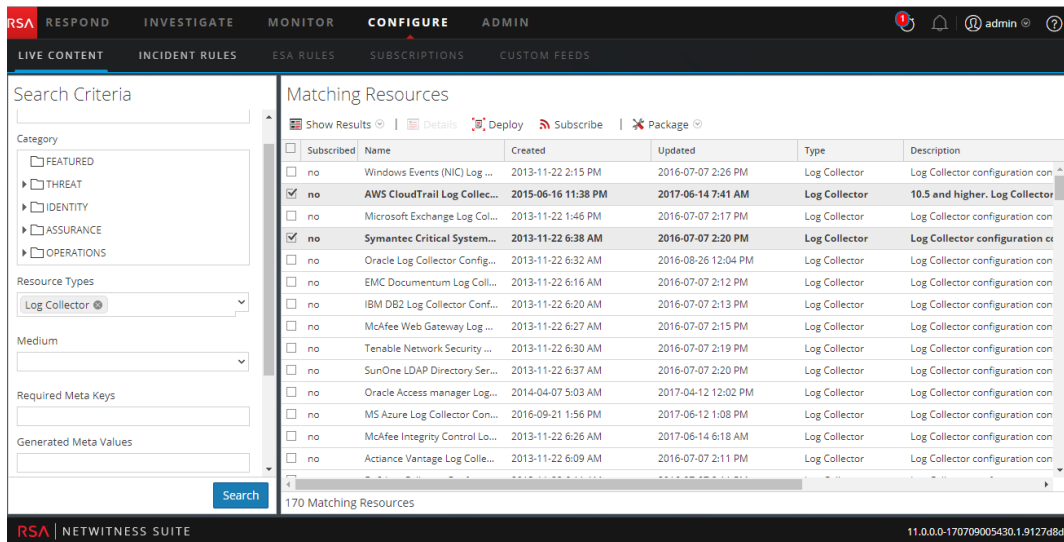
3. Restart the Log Decoder service. In the Services view, click   > **Restart**.

### Deploy a Log Decoder Feed in Live

To deploy the feed in the live environment:

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:

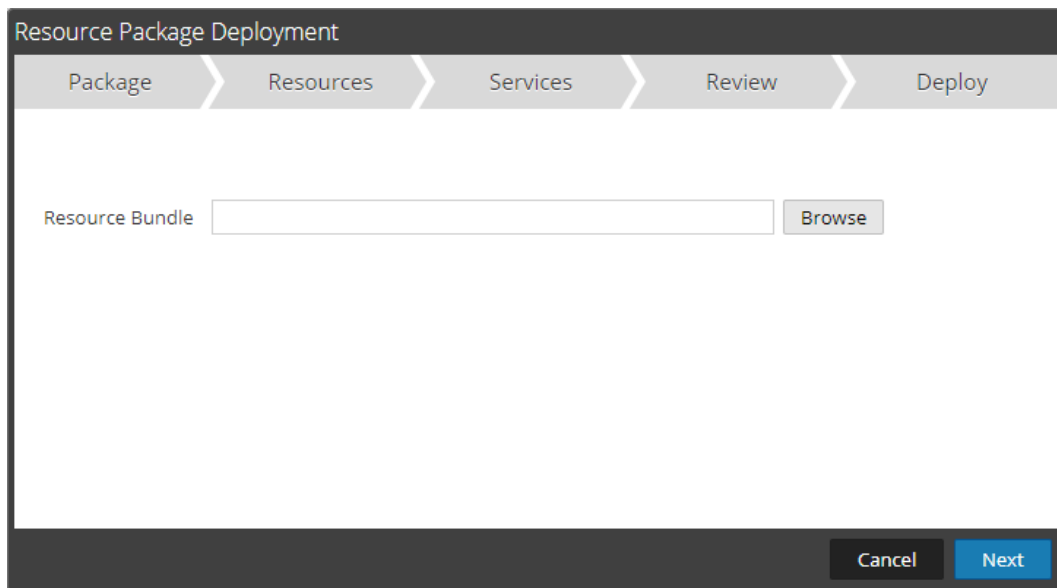
- a. In the **Live Search View**, browse Live resource (for example, search for the **Log Collector** resource Type).
- b. In the **Matching Resources** panel, select **Show Results > Grid**.
- c. Select the checkbox to the left of the resources that you want to deploy.



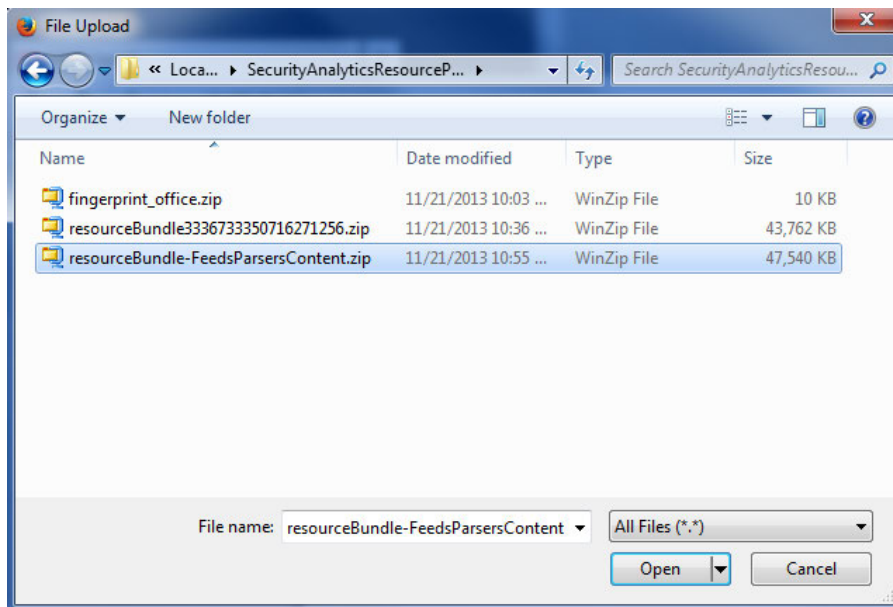
- d. In the Matching Resources toolbar, click  **Deploy**

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.

3. Click **Next**.

The **Services** page is displayed that 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.

4. 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.

Deployment Wizard

Resources Services Review Deploy

Services Groups

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

Cancel Previous Next

5. Click **Next**.

The **Review** page is displayed.



Deployment Wizard				
Resources		Services	Review	Deploy
Service	Service Type	Resource Name	Resource Type	
SA UI Endpoint	SA Local	Basic Rule Template	RSA Event Stream Analy...	

Cancel Previous Deploy

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

6. Click **Deploy**.

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

Deployment Wizard

Resources

Services

Review

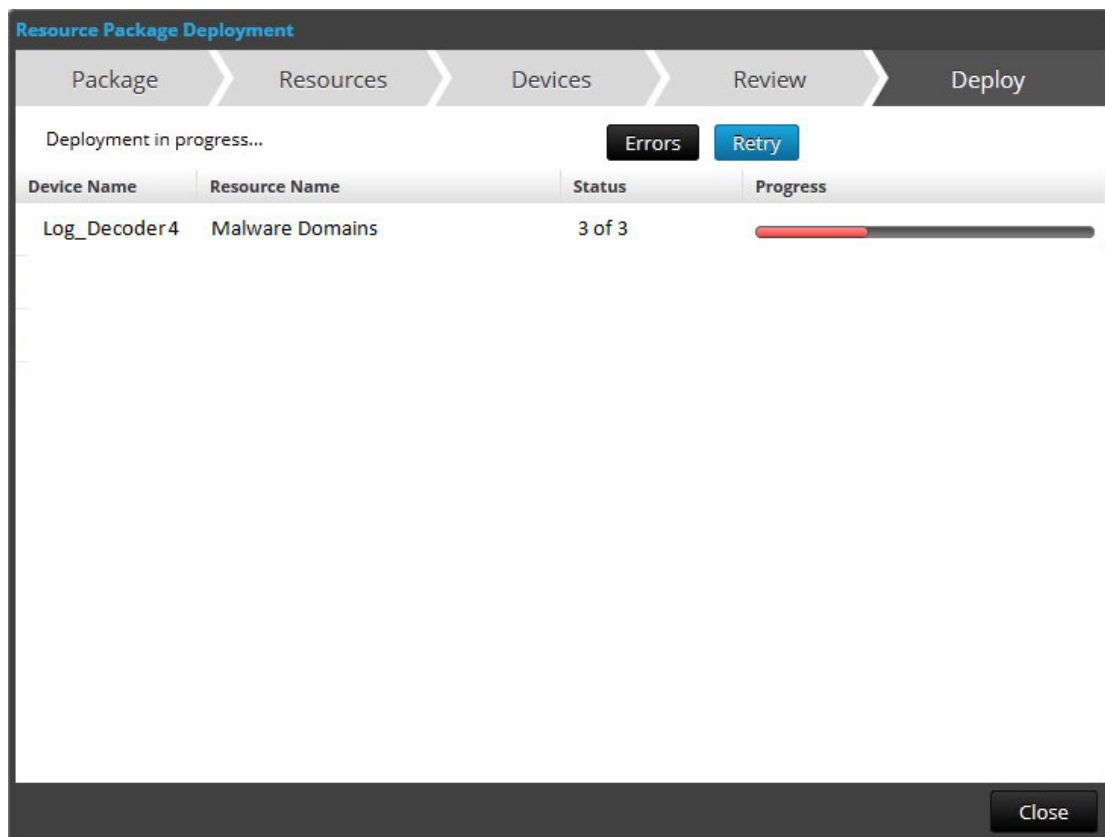
Deploy

Live deployment task finished successfully

Service Name	Resource Name	Status	Progress
SA UI Endpoint	Basic Rule Template	1 of 1	<div></div>

Close

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.




7. Click **Close**.

**Note:** The Source IP should be indexed by selecting the type as 'IP' as the ip.src. and ip.dst are in IPv4 format.

In this scenario, a custom meta key location.src (location source) is added by indexing the hostname (alias.host). In this example, the printer hostname are populated in meta key 'alias.host'. So, select 'alias.host' as callback key, and index type as 'Non IP' in the Feed Wizard as shown below. In the Define Values section, select the custom meta key from the drop down menu.

### Add the Custom Meta Key Entry in the Concentrator Custom Index file

To add the custom meta entry in the concentrator custom index file:

1. Go to **ADMIN > Services > Concentrator**.
2. Click  > **View > Config > Files tab > index-concentrator-custom.xml**.
3. Add the custom meta key entry in the Concentrator index file.

```
<Language>
  <?xml version="1.0" encoding="utf-8"?>
  <Language level="IndexNone" defaultAction="Auto">
    <!-- Reserved Meta key for Feed -->
    <Key description="Source Location" level="IndexValues"
name="location.src" format="Text" valueMax="10000"
defaultAction="Open"/>
  </Language>
```

4. To restart the Concentrator service, in the Services view, click   > **Restart**.



**Note:** In case of the Broker, the Broker derives its index from the Concentrator from which it aggregates. So you do not need to create custom meta in the broker. If you have not indexed the meta key in the concentrator, the broker will not display in the investigation.


## Investigate on the Custom Meta Key

**Note:** You have to log out and log in from the NetWitness Suite User Interface, before you can view the custom meta key in Investigation.



To investigate on the custom meta key:


1. Go to **INVESTIGATE > Navigate**.
2. Select a Concentrator service, and click **Navigate**.

**Hostname Aliases** (3 values) 

printer3 (1) - printer2 (1) - printer1 (1)

**Source Location** (3 values) 

sixth floor a wing (1) - fifth floor c wing (1) - fifth floor b wing (1)

Here is an example of a report executed on the concentrator.

Asset Source Location

Generated on - 2015-10-29 06:44 (UTC)

2015

10  
27

06:44:00 (UTC)

Time Range

2015

10  
29

06:43:59 (UTC)

Source Location /SITPRD-HYBLD1 - Concentrator

	Hostname Aliases	Source Location
1	<a href="#">PRINTER3</a>	<a href="#">SIXTH FLOOR A WING</a>
2	<a href="#">PRINTER1</a>	<a href="#">FIFTH FLOOR B WING</a>
3	<a href="#">PRINTER2</a>	<a href="#">FIFTH FLOOR C WING</a>
4	<a href="#">PRINTER2</a>	<a href="#">FIFTH FLOOR C WING</a>
5	<a href="#">PRINTER3</a>	<a href="#">SIXTH FLOOR A WING</a>
6	<a href="#">PRINTER1</a>	<a href="#">FIFTH FLOOR B WING</a>
7	<a href="#">PRINTER2</a>	<a href="#">FIFTH FLOOR C WING</a>
8	<a href="#">PRINTER3</a>	<a href="#">SIXTH FLOOR A WING</a>
9	<a href="#">PRINTER1</a>	<a href="#">FIFTH FLOOR B WING</a>
10	<a href="#">PRINTER1</a>	<a href="#">FIFTH FLOOR B WING</a>

## Additional Procedures

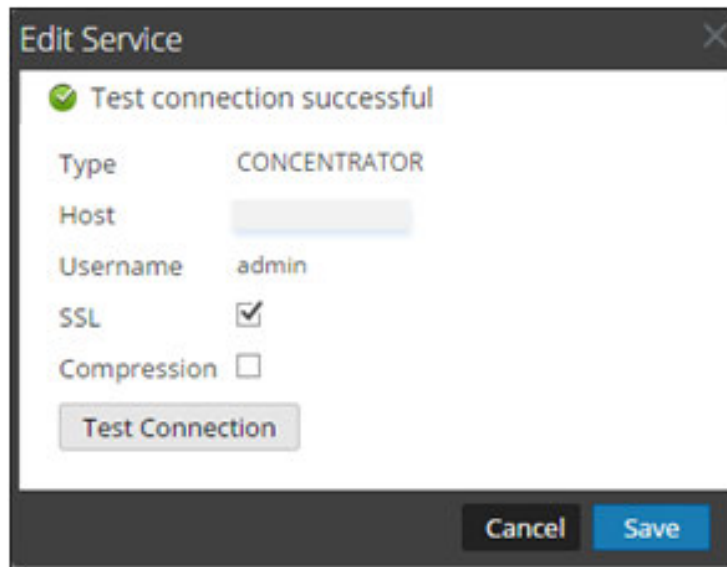
The following procedures must be executed if you have Warehouse Connector, Archiver, Reporting Engine and ESA configured.

### Update the Schema in ESA

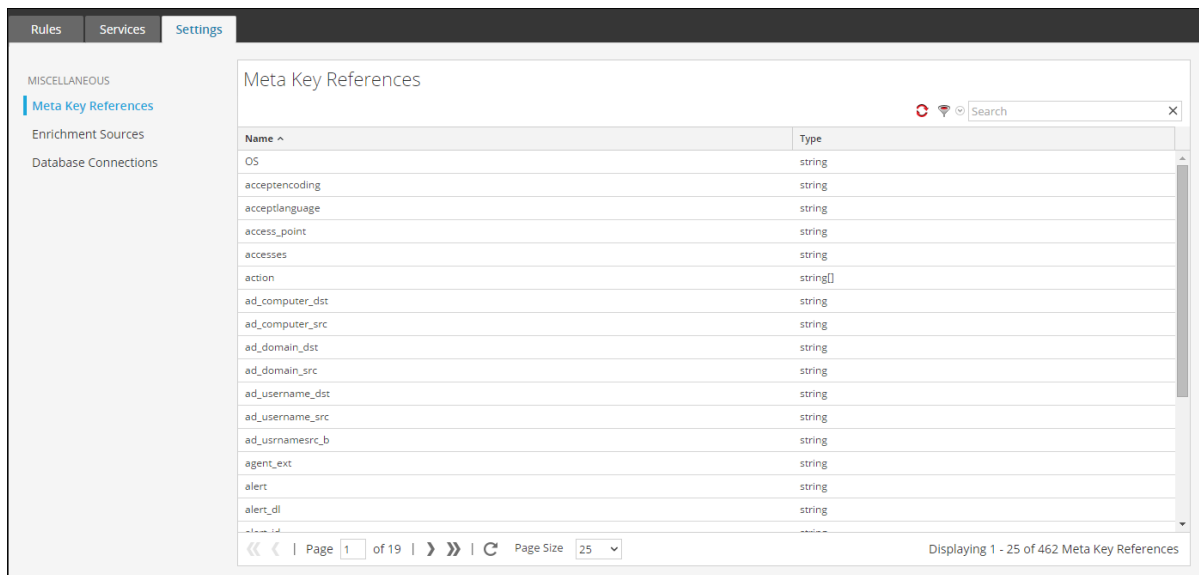
Before you update the schema in ESA, the custom meta key should be indexed in the concentrator.

To update the schema ESA rules and to be able to use the new custom meta keys:

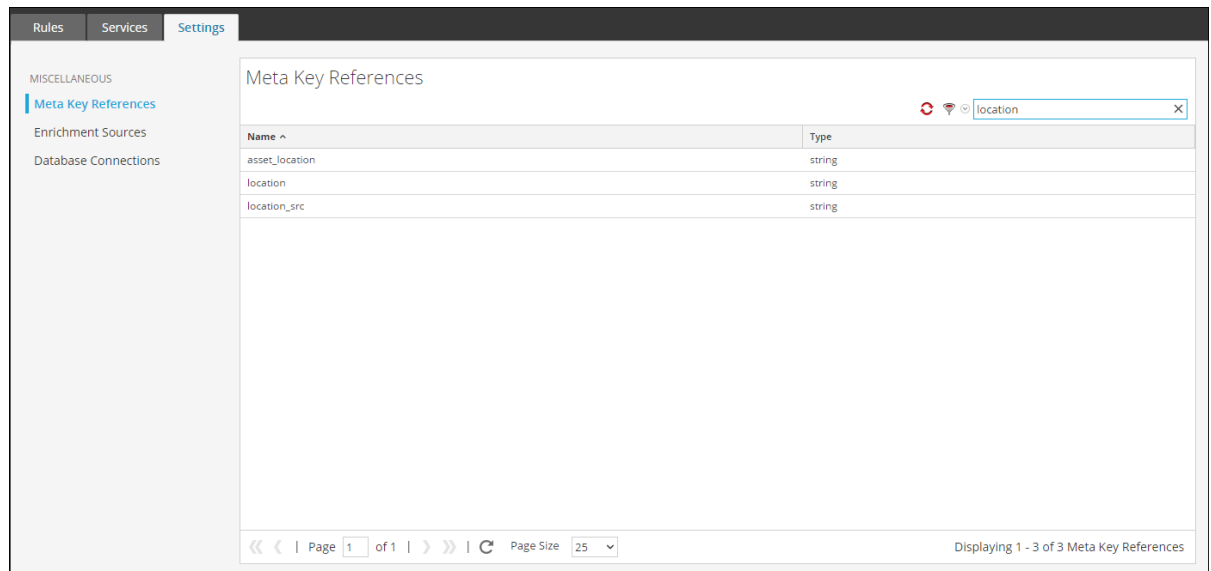
1. Go to **ADMIN > Services > ESA- Event Stream Analysis > View > Config**.
2. Edit the Concentrator Datasource.
3. Click **Test Connection**.



4. Click **Save** after the connection is successful.
5. Click **Apply**.
6. Navigate to **Alerts > Configure > Settings**.



7. Click the **Search** tab and search for the name of the custom meta key.  
The custom meta key name and type is displayed.



### Update the Schema in Archiver

If you want to configure the Archiver, using the new custom meta keys, you need to update the Archiver schema in the Reporting Engine. To update the Archiver schema in Reporting Engine:

1. Go to **ADMIN > Services > Archiver**.
2. Select > **View > Config > Files > index-archiver-custom.xml**.
3. Add the custom meta key entry in the Archiver index file.

```
<Language>
  <?xml version="1.0" encoding="utf-8"?>
  <Language level="IndexNone" defaultAction="Auto">
    <!-- Reserved Meta key for Feed -->
    <Key description="Source Location" level="IndexValues"
name="location.src" format="Text"
  valueMax="10000" defaultAction="Open"/>
  </Language>
```

4. To restart the Archiver service, click > **Restart**.

The Archiver schema is updated with the custom meta key.

### Update the Schema in Warehouse Connector

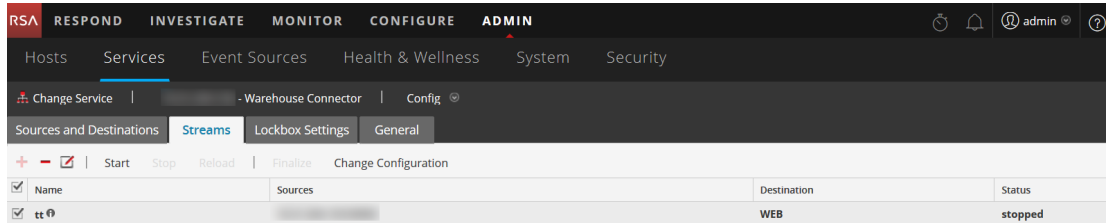
If you want to configure the Warehouse with custom meta and use it in warehouse report then you need to update the Warehouse schema in the Reporting Engine.

If the Log Decoder or Decoder, where the custom meta key is added, is one of the sources in the Warehouse Connector stream, you need to update the schema in the Warehouse Connector.

To update the Warehouse schema in the Reporting Engine:

1. Go to **ADMIN > Services > Warehouse Connector**.
2. Click  > **View > Config > Files** tab > **index-logdecoder-custom.xml**.
3. Select the stream and click **Reload**.


The warehouse connector pulls the schema from the downstream devices (Log Decoder/Decoder).



For more information on streams, see "Configure Streams" in the *Warehouse Connector Configuration Guide*.


### Update the Schema in Reporting Engine

To update the schema in Reporting Engine:

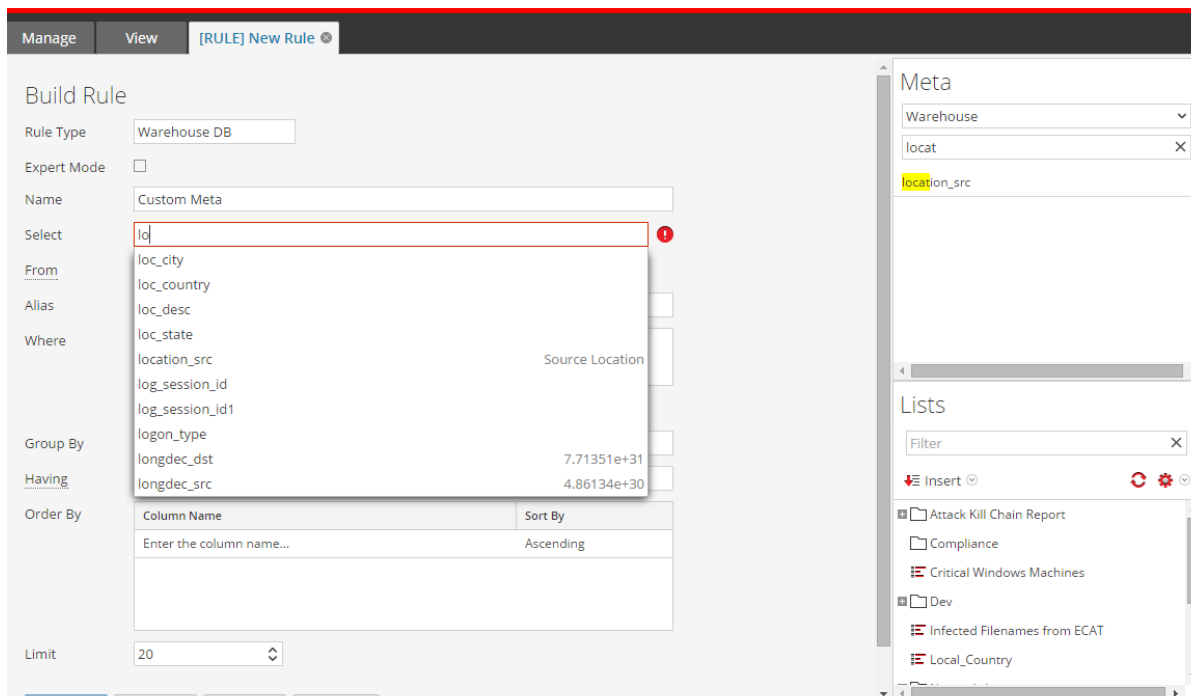
1. Go to **ADMIN > Services > Reporting Engine**.
2. Click  > **Restart**.

**Note:** Restart the Reporting Engine or wait for thirty minutes for the schema to be updated.

To view the custom meta key:

1. Navigate to **Reports > Rules**.
2. In the toolbar, click .
3. Select **Warehouse DB**.
4. In the Build Rule tab, search for the custom meta from the right panel.  
The custom meta key is displayed.





## Upload and Delete Custom Parsers

RSA NetWitness Suite has the ability to upload parsers from your local system and delete these parsers.

### Upload Parsers to a Decoder or Log Decoder

The Upload option in the Service Config view > Parsers tab displays the Upload Parsers dialog, in which you can manage the uploading of parsers to a Decoder or Log Decoder. In the File list, you prepare a list of parsers for uploading. You can add files from a directory structure, and delete files from the list if you decide that you don't want to upload a particular file. When the list is ready, clicking Upload starts the upload process.

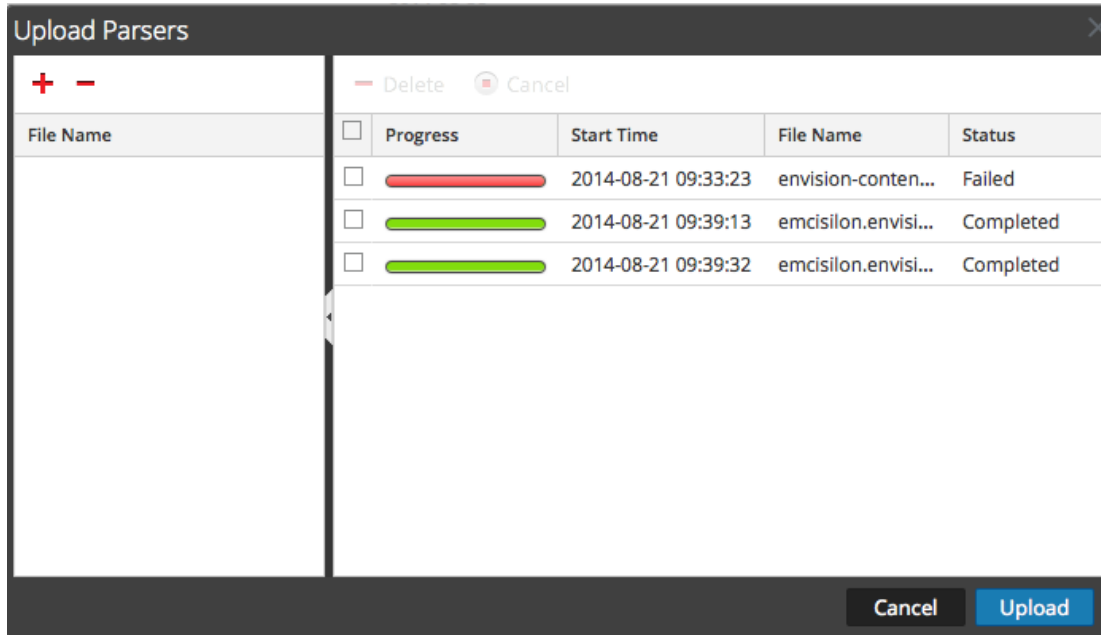
1. Go to **ADMIN > Services**, select a service, and > **View > Config**.

The Config view for the selected service is displayed.

2. Click the **Parsers** tab.

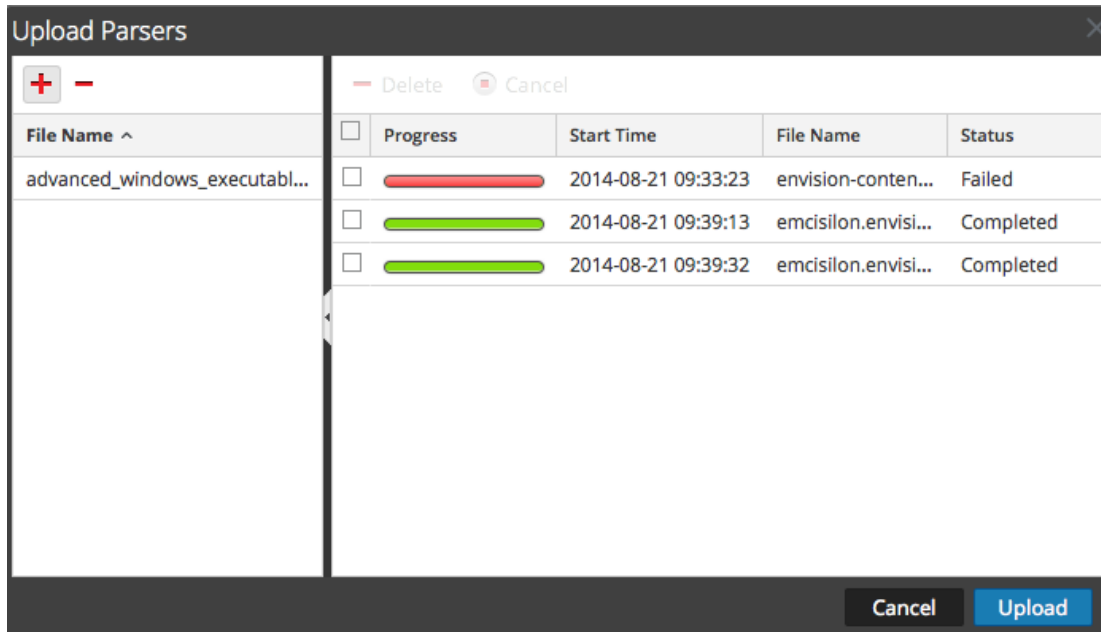
- Click  **Upload**.

The Upload Parsers dialog is displayed.



- Click **+**.
- Select the **.flex**, **.parser**, and **.lua** files to be updated, and click **Open**.

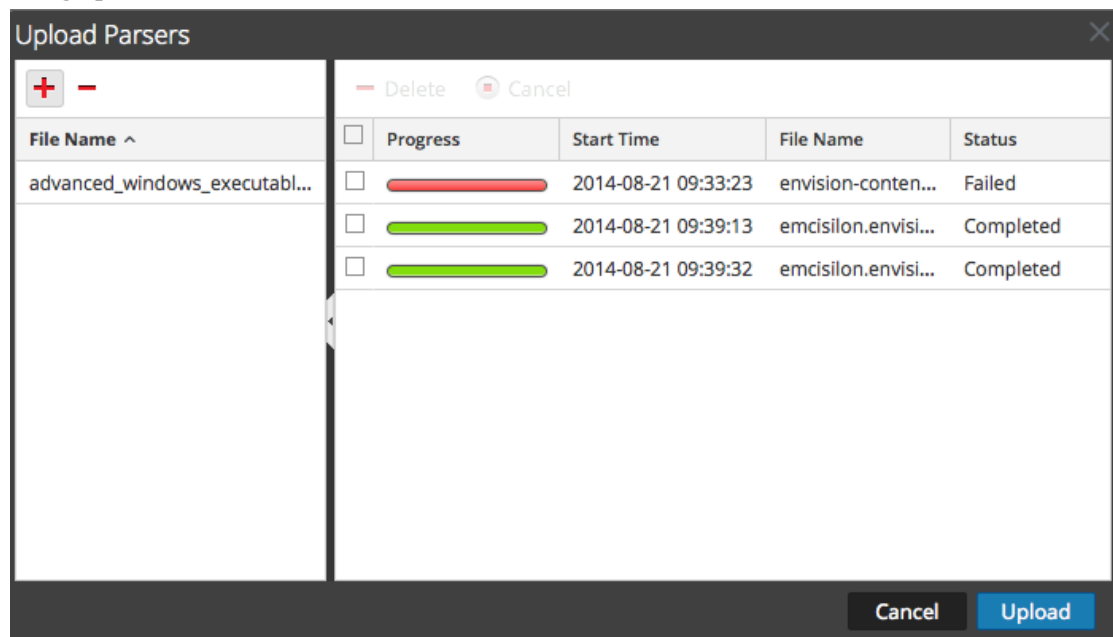
The dialog closes, and the selected files are displayed in the File list.



- Click **Upload**.

The Upload Job grid shows the progress of the upload jobs with each job representing a file

being uploaded.



- Use any of the Upload grid tools to manage the upload of selected jobs: pause and resume, cancel, and delete.

Once a job is complete, it is deployed on the Decoder and listed with the deployed parsers in Parsers tab.

## Manage Upload Jobs

You can use any of the Upload grid tools to manage the upload of selected jobs: pause, resume, cancel, and delete.



- To cancel uploading a set of parsers while the upload is in queue or progress, click **Cancel**.
- To pause uploading a set of parsers, if the upload is not yet complete, click **Pause**.
- To resume uploading a set of parsers after a pause, click **Resume**.
- To delete an upload job, click .

## Delete Deployed Parsers

The Delete option in the Service Config view > Parsers tab provides a way to delete deployed parsers from a Decoder or Log Decoder. Parsers can be added and removed while a Decoder is running without affecting capture.

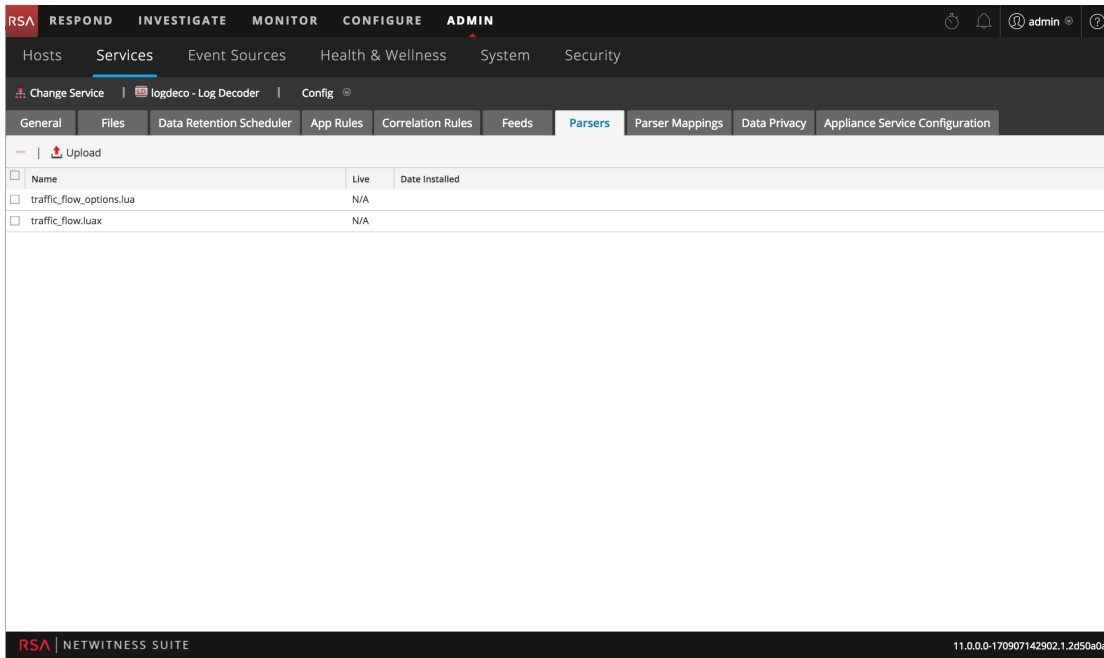
**Note:** Unless otherwise stated, any reference to Decoders applies to Log Decoders as well.


To delete a parser from a Decoder:

1. Go to **ADMIN > Services**, elect a service, and   > **View > Config**.

The Services Config view for the selected service is displayed.

2. Click the **Parsers** tab.



3. In the **Parsers** tab, select one or more parsers to delete.
  4. Click .
- A dialog requests confirmation that you want to delete the parsers.
5. If you want to delete the parsers, click **Yes**.
- The parsers are removed from the Decoder immediately.

## Enable and Configure the Entropy Parser

Beginning with NetWitness Suite 11.0, the administrator can configure a Decoder to use a NetWitness native parser, known as the Entropy parser. When the Entropy parser is enabled, analysts have visibility into channels that are trying to blend in with other traffic, but do not follow normal protocol behavior. This helps to identify channels that do not conform to the normal environment traffic baseline, and may, therefore, be worthy of investigation.

The parser creates meta keys, based on statistics collected by the native NetWitness Suite parser, that help to identify behavior of any channel that is getting lots of network traffic. When the parser is first enabled, the analyst needs to become familiar with overall behavior for the different channels seen in a captured session to understand the frequency of bytes and the normal client and server payload. Once the normal behavior is known, analysts can use the meta keys to find behavior that does not match the expected.

By default, the Entropy parser generates 10 additional meta keys that do not add significantly to the load on a Decoder, and are useful for this specialized case. The parser is disabled by default.

Enable indexing if you have interest in exploring interesting sessions based on payload byte analysis of the packets. By default, to make indexing easier, the normal `Float32` value for `entropy.req` and `entropy.res` is multiplied by 10k and stored in a `UInt16` (thus giving four digits of precision, 0 to 10,000).

However, if you define the `entropy.*` fields in the Decoder language to be `Float32`, the Decoder will store it as a float with a range of 0.0 to 1.0. Take care to change the language everywhere if you decide to keep it as a `Float32`.

RSA does not recommend indexing as a `Float32` because of the high unique counts due to minute changes in precision.

These are the 10 new meta keys generated by the Entropy parser by default:

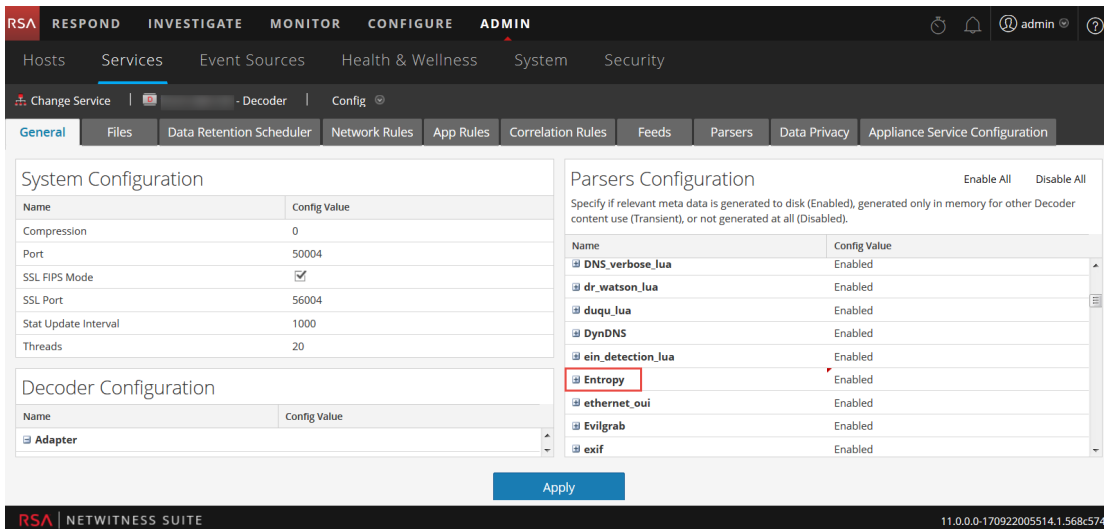
- `entropy.req` and `entropy.res`: These meta keys capture entropy using the Shannon entropy equation, which has a floating point value as a result. The floating point value of 0 to 1.000 is multiplied by 10000 and written in NetWitness Suite Suite as `UInt 16`, an unsigned integer of 0 through 10000. .
- `mcb.req` and `mcb.res`: The most common byte is simply which byte for each side (0 thru 255) was seen the most.
- `mcbc.req` and `mcbc.res`: The most common byte count is the number of times the most common byte (above) was seen in the session streams.
- `ubc.req` and `ubc.res`: - Unique byte count is the number of unique bytes seen in each stream. 256 would mean all byte values of 0 thru 255 were seen at least once.
- `payload.req` and `payload.res`: The payload size metrics are the payload sizes of each session side at the time of parsing. However, in order to keep indexing from having high unique counts (bad for performance), the two payload size metas below are calculated this way:
  - Less than 1000 is the exact number of payload bytes.
  - 1000 or greater is bucketed in increments of 1000. So a size of 5826 would be stored as 5000.

To enable and configure the Entropy parser on a Decoder

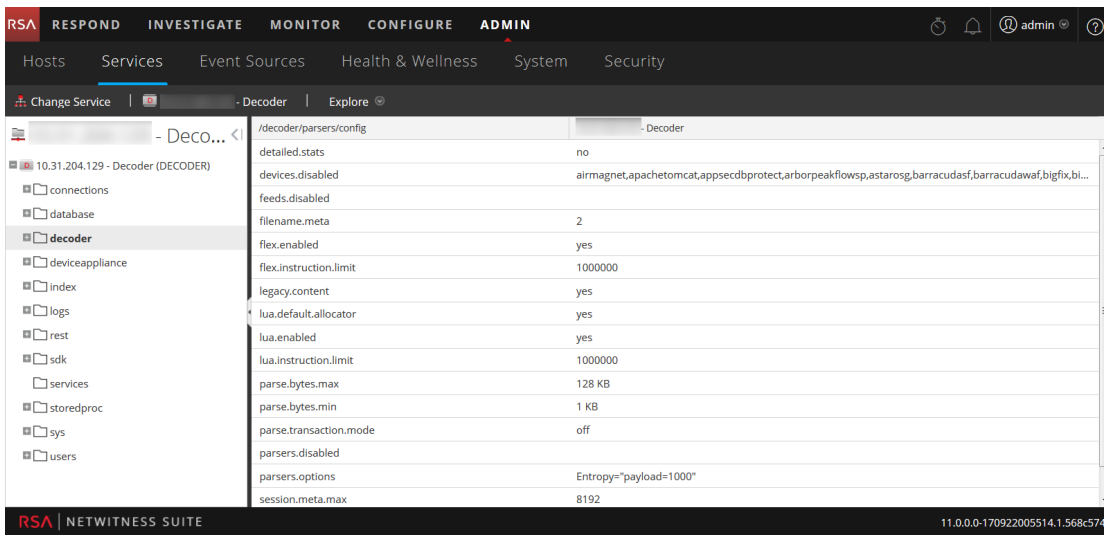
1. Log in to RSA NetWitness, and select **ADMIN > Services** in the NetWitness Suite menu.
2. In the Services view, select the Decoder that you want to configure, and then **View > Config**.

The Services Config view for the selected Decoder is displayed.

- The Entropy parser is disabled by default. Click the drop-down list under **Config Value** and select **Enabled**. If you want to disable some of the meta keys, click the drop-down list and select **Disabled** next to the meta key.



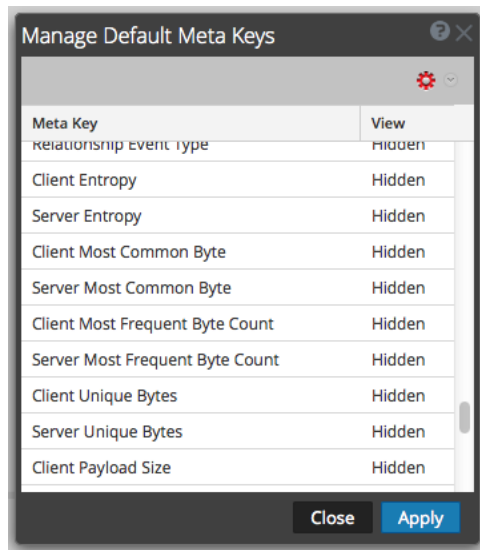
- Click **Apply**
- The Entropy parser is enabled and begins creating the new meta keys as configured in the Concentrator custom index file.
- Navigate to the **Explore View** for the Decoder, and select the **decoder > parsers > config** node. In the parsers.options, you can set the Entropy parser payload. The default value shown in the screen capture is `Entropy = payload = 1000`. When defining the value, the syntax is `Entropy = payload = "1000"`. The quotes are required if there is white space in the value, and it is a good practice to always use them to avoid white space issues. If you want to see the exact payload, set this parameter to "1".



The default Entropy payload is 1000, which means that if the payload count is less than 1000,

the exact value is provided. If the payload count is greater than 1000, the value is rounded down to the nearest 1000. For example, a count of 3798 is rounded down to 3000.

6. If you want to change the default Entropy payload rounding factor, edit the value. This change takes effect when the parser is reloaded
7. In the Service Config view select the Concentrator that is aggregating traffic from this Decoder. Select **View > Files** and open the Custom Index file for the Concentrator. Look for the Entropy parser meta keys to see if they are included and uncommented.  
By default the keys are commented out and therefore not enabled. To enable that part of the language the administrator needs to copy that part of index file into the `index-concentrator-custom.xml` and uncomment the key description line for each meta key. An example of the custom index file with the Entropy parser keys and instructions is shown below.
8. With the Entropy meta keys enabled, they are available to analysts in Investigate, but hidden by default. To make the meta keys visible in the Investigate Values view, edit the default meta keys in the Default Meta Keys dialog so that they are open instead of hidden. You can manage these meta key the same way you manage other meta keys.



### Entropy Parser Configuration in the Concentrator Custom Index File

The following is an excerpt of the Concentrator Index file lines that the administrator must copy to the custom index file. The comments provide guidance on configuring the parser.

<!-- This section is commented out because it's only used by the Entropy parser which is disabled by default. To enable this part of the language, copy to index-concentrator-custom.xml and uncomment the keys. HOWEVER, take note that depending on how the Entropy parser is configured, the entropy.req and entropy.res format might be a Float32 instead of a UInt16. So make sure to change to the correct type if necessary.-->

<!-- Entropy parser meta - enable indexing if you have interest in exploring this for interesting sessions based on payload byte analysis of the packets. By default, to make indexing easier, the normal Float32 value for entropy.res and entropy.req is multiplied by 10k and stored in a UInt16 (thus giving 4 digits of precision, 0 to 10,000). However, if you define the \*.entropy fields in the Decoder language to be Float32, it will store it as a float with a range of 0.0 to 1.0. Take care to change the language everywhere if you decide to keep it as a Float32. We also don't recommend indexing as a Float32.-->

<!--

<key description="Client Entropy" format="UInt16" level="IndexNone" name="entropy.req" valueMax="10001"/>

<key description="Server Entropy" format="UInt16" level="IndexNone" name="entropy.res" valueMax="10001"/>

-->

<!-- The most common byte is simply which byte for each side (0 thru 255) was seen the most -->

<!--

<key description="Client Most Common Byte" format="UInt8" level="IndexNone" name="mcb.req"/>

<key description="Server Most Common Byte" format="UInt8" level="IndexNone" name="mcb.res"/>

-->

<!-- The most frequent byte count is the number of times the most common byte was seen in the session streams -->

<!--

<key description="Client Most Frequent Byte Count" format="UInt32" level="IndexNone" name="mcbc.req" valueMax="500000"/>

<key description="Server Most Frequent Byte Count" format="UInt32" level="IndexNone" name="mcbc.res" valueMax="500000"/>

-->

<!-- Unique byte count is the number of unique bytes seen in each stream. 256 would mean all byte values of 0 thru 255 were seen at least once -->

<!--

<key description="Client Unique Bytes" format="UInt16" level="IndexNone" name="ubc.req"/>

<key description="Server Unique Bytes" format="UInt16" level="IndexNone" name="ubc.res"/>

-->



<!-- The payload size metrics are the payload sizes of each session side at the time of parsing. However, in order to keep indexing from having high unique counts (bad for performance), the two payload size meta values below are calculated like so:

Less than 1000 is the exact number of payload bytes

1000 or greater is bucketed in increments of 1000. So a size of 5826 would be stored as 5000. -->

<!--

<key description="Client Payload Size" format="UInt32" level="IndexNone" name="payload.req" valueMax="500000"/>

<key description="Server Payload Size" format="UInt32" level="IndexNone" name="payload.res" valueMax="500000"/>

-->

## Decoder and Log Decoder Additional Procedures

---

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

### Topics

- [Configure 10G Capability](#)
- [Configure a Log Decoder to Accept Protobuf](#)
- [Configure Session Split Timeouts](#)
- [Configure Syslog Forwarding to Destination](#)
- [Configure Transaction Handling on a Decoder](#)
- [Create Custom Meta Keys Using a Custom Feed](#)
- [Decrypt Incoming Packets](#)
- [Edit Decoder System Configuration](#)
- [Enable CPU Usage Statistics for Installed Content](#)
- [Enable Parser Mappings](#)
- [Enable or Disable Lua and Flex Parsing Systems](#)
- [Map IP Address to Service Type for Log Parsing](#)
- [Obtain Log Files a from Pre-11.0 Log Decoder](#)
- [Upload a Log File to a Log Decoder](#)
- [Upload a Packet Capture File](#)

## Configure 10G Capability

This topic guides administrators in how to tune a Packet Decoder specifically for high speed packet capture using NetWitness Suite 11.0. This applies when capturing packets on a 10G interface card. Packet capture at high speeds requires careful configuration and pushes the Decoder hardware to its limits, so please read this entire topic when implementing a 10G capture solution.

RSA NetWitness Suite provides support for high-speed collection on the Decoder. You can capture network packet data from higher speed networks and optimize your Packet Decoder to capture network traffic up to 8Gb/sec sustained and 10Gb/sec burst, depending on which parsers and feeds you have enabled.

Enhancements that facilitate capture in these environments include the following:

- Utilization of the `pf_ring` capture driver capability to leverage the commodity 10G Intel NIC card for high-speed capture.
- Introduction of `assembler.parse.valve` configuration, which automatically disables application parsers when certain thresholds are exceeded, to limit risk of packet loss. When the application parsers are disabled, network layer parsers are still active. When stats fall below exceeded thresholds, application parsers are automatically re-enabled.

## Hardware Prerequisites

- A Series 4S or Series 5 Decoder
- An Intel 82599-based ethernet card, such as the Intel x520. All RSA-provided 10G cards meet this requirement. Two examples are:
  - All SMC-10GE cards provided by RSA.
  - A Dell Network Daughter Card using an Intel controller to provide 10G network interfaces. This is included in all Series 5 hardware.
- For the Series 4S / Dell R620 only: 96 GB of DD3-1600 memory in **dual-rank** DIMMs. Single-rank DIMMs may decrease performance by as much as 10%. To determine the speed and rank of the installed DIMMs, run this command:  

```
dmidecode -t 17.
```
- Sufficiently large and fast storage to meet the capture requirement. Storage considerations are covered later in this topic.
- Each Packet Decoder configured with a minimum of 2 DACs or SAN connectivity.

## Software Prerequisites

- Dell R620-based systems, such as the Series 4S, must have their BIOS updated to v1.2.6 or later.
- The 10G Decoder capability is only supported on RSA-provided Decoder Installation images. All required software is installed by default.
- If upgrading from a previous release, perform the upgrade first before proceeding with configuration

## Install the 10G Decoder

**Note:** You can skip to "Configure the 10G Decoder" if you are starting with new Series 5 hardware.

Perform the following steps to install the NetWitness 10G Decoder:

### Download and Update the BIOS

**Note:** BIOS revisions earlier than v1.2.6 have issues properly identifying the location of the 10G capture card within the system. It is recommended that customers update to the latest v2.2.3 BIOS, but is not required for 10G if they are running v1.2.6 or later.

1. Download BIOS v2.2.3 from the following location:  
<http://www.dell.com/support/home/us/en/19/Drivers/DriversDetails?driverId=V7P04>
2. Download the Update Package for the Red Hat Linux file.
3. Copy the file to the NetWitness server.
4. Login as `root`.
5. Change the permissions on the file to execute.
6. Run the following file:  

```
./BIOS_V7P04_LN_2.2.3.BIN
```
7. Reboot the system when execution is complete and a reboot is requested.

**Note:** The BIOS installation procedure takes approximately 10 minutes.

### Locate the 10G Decoder Packages

The packages required to configure the 10G Decoder should already be present on the Decoder installation image. You should not have to install any additional packages. The packages that provide the 10G driver capability are:

- `pfring-dkms-6.5.0-6.rpm`
- `ixgbe-zc-4.1.5.6-dkms.noarch.rpm`

### Verify 10G Decoder Packages Are Installed

Installation of the 10G Decoder packages is handled automatically. Therefore, there should be no action to enable the 10G functionality.

- If you upgraded the kernel packages as part of an upgrade, a reboot is required. The operating system will recompile and install the drivers for the upgraded kernel.
- You can verify that the installation was successful if you see additional `PFRINGZC` interfaces available when selecting the Capture Port Adapter as described below.

### Configure the 10G Decoder

Perform the following steps to configure the 10G Decoder:

1. From the **Decoder Explorer** view, right-click **Decoder** and select **Properties**.
2. In the properties drop-down menu, select **reconfig** and enter the following parameters:  
`update=1 op=10g`  
This adjusts the Decoder packet processing pipeline to allow for higher raw data throughput, but less parsing ability.
3. From the **Decoder Explorer** view, right-click **database** and select **Properties**.
4. In the **Properties** drop-down menu, select **reconfig** and enter the following parameters:  
`update=1 op=10g`  
This adjusts the packet database to use very large file sizes and Direct I/O.
5. Select the capture port adapter. Options for this include:
  - Single port capture - **PFRINGZC,p1p1** or **PFRINGZC,p1p2**
  - Capture off both ports – Select **PFRINGZC,P1P1** and in the **Explorer** view, set  
`capture.device.params = device=zc:p1p2,zc:p1p1`
6. If the write thread is having trouble sustaining the capture speed, you can try the following:  
Change `/datebase/config/packet.integrity.flush` to `normal`.

**Note:** You can adjust the `packet.file.size` to a higher value, but keep the file size under 10 GB, as the whole file is buffered in memory.

7. (Optional) Application parsing is extremely CPU intensive and can cause the Decoder to drop packets. To mitigate application parsing-induced drops, you can set

`/decoder/config/assembler.parse.valve` to true. These are the results:

- When session parsing becomes a bottleneck, application parsers (HTTP, SMTP, FTP, and others) are temporarily disabled.
  - Sessions are not dropped when the application parsers are disabled, just the fidelity of the parsing performed on those sessions.
  - Sessions parsed when the application parsers are disabled still have associated network meta (from the network parser).
  - The statistic `/decoder/parsers/stats/blowoff.count` displays the count of all sessions that bypassed application parsers (network parsing is still performed).
  - When session parsing is no longer a potential bottleneck, the application parsers are automatically re-enabled.
  - The assembler session pool should be large enough that it is not forcing sessions.
  - You can determine if sessions are being forced by the statistic `/decoder/stats/assembler.sessions.forced` (it will be increasing). Also `/decoder/stats/assembler.sessions` will be within several hundred of `/decoder/config/assembler.session.pool`.
8. (Optional) If you need to adjust the MTU for capture, add the `snaplen` parameter to `capture.device.params`. Unlike previous releases, the `snaplen` does not need to be rounded up to any specific boundary. The Decoder automatically adjusts the MTU set on the capture interfaces.
  9. The following configuration parameters are deprecated and no longer necessary
    - The `core=` parameter in `capture.device.params`
    - Any configuration files under `/etc/pf_ring` directory

**Note:** An Ethernet device installed post imaging does not require any configuration for use as a capture device. It does require configuration if it is used as a network interface, or for system tools to access it without manual configuration.

### Typical Configuration Parameters

Typical configuration parameters are listed below. Actual parameters may vary depending on the amount of memory and CPU resources available.

1. session and packet pool settings(under `/decoder/config`):
  - `pool.packet.pages = 1000000`
  - `pool.session.pages = 300000`

2. Packet write block size under (`/database/config/packet.write.block size`) set to `filesize`.

**Note:** This configures the Decoder to buffer the file with huge pages and write using direct I/O for maximum performance.

3. Parse Thread Count (under `/decoder/config`).

```
parse.threads =12
```

## Storage Considerations

When capturing at 10G line rates, the storage system holding the packet and meta databases must be capable of sustained write throughput of 1400 MBytes/s.

### Using the Series 4S Hardware (With Two or More DAC Units)

The Series 4S is equipped with a hardware RAID SAS controller capable of an aggregate 48Gbit/s of I/O throughput. It is equipped with eight external 6 Gbit ports, organized into two 4-lane SAS cables. The recommended configuration for 10G is to balance at least two DAC units across these two external connectors. For example, connect one DAC to one port on SAS card, and then connect another DAC to the other port on the SAS card.

For environments with more than two DACs, chain them off each port in a balanced manner. This may require re-cabling of DACs in an existing deployment, but should not affect data that has already been captured on the Decoder.

If adding new capacity, use the currently available `NwMakeArray` script to provision the DAC units. The script automatically adds one DAC per execution (that means, if adding three DACs, then the script must be run three times), adding the DACs to the `NwDecoder10G` configuration as separate mount points. The independent mount points are important, as this configuration allows the `NwDecoder10G` to segregate write I/O from capture from the read I/O needed to satisfy packet content requests.

### Using SAN and Other Storage Configurations

The Decoder allows any storage configuration that can meet the sustained throughput requirement. The standard 8-Gbit FC link to a SAN is not sufficient to store packet data at 10G; in order to use a SAN it may be required to perform aggregation across multiple targets using a software-RAID Scheme. Thus environments using SAN are required to configure connectivity to the SAN using multiple FCs.

## Parsing and Content Considerations

Parsing raw packets at high speeds presents unique challenges. Given the high session and packet rates, parsing efficiency is paramount. A single parser that is inefficient (spends too long examining packets) can slow the whole system down to the point where packets are dropped at the card.

For initial 10G testing, start with only native parsers (except SMB/WebMail). Use the native parsers to establish baseline performance and with little to no packet drops. Do not download any Live content until this has been done and the system is proven to capture without issue at high speeds.

After the system has been operational and running smoothly, Live content should be added very slowly - especially parsers.

### **Best Practices**

Whether you are updating a currently deployed system or deploying a new system, it is recommended you use the following best practices to minimize risk for packet loss. One caveat is if you are updating a current 10G deployment but not adding any additional traffic. For example, a current Decoder capturing off a 10G card at 2G sustained should see no difference in performance, unless part of the update also entails adding additional traffic for capture.

- Incorporate baseline parsers (except SMB/Webmail, both of which generally have high CPU utilization) and monitor to ensure little to no packet loss.
- When adding additional parsers, add only one or two parsers at a time.
- Measure performance impact of newly added content, especially during peak traffic periods.
- If drops start occurring when they did not happen before, disable all newly-added parsers and enable just one at a time and measure the impact. This helps pinpoint individual parsers causing detrimental effects on performance. It may be possible to refactor it to perform better or reduce its feature set to just what is necessary for the customer use case.
- Although lesser performance impacts, feeds should also be reviewed and added in a phased approach to help measure performance impacts.
- Application Rules also tend to have little observable impact, though again, it is best not to add a large number of rules at once without measuring the performance impact.

Finally, making the recommended configuration changes outlined in the Configuration section will help minimize potential issues.

### **Tested Live Content**

All (not each) of the following parsers can run at 10G on the test data set used:

- MA content (7 Lua parsers, 1 feed, 1 application rule)
- 4 feeds (alert ids info, nwmalwaredomains, warning, and suspicious)
- 41 application rules
- DNS\_verbose\_lua (disable DNS)



- fingerprint\_javascript\_lua
- fingerprint\_pdf\_lua
- fingerprint\_rar\_lua
- fingerprint\_rtf\_lua
- MAIL\_lua (disable MAIL)
- SNMP\_lua (disable SNMP)
- spectrum\_lua
- SSH\_lua (disable SSH)
- TLS\_lua
- windows\_command\_shell
- windows\_executable

NOT TESTED:

- SMB\_lua, native SMB disabled by default
- html\_threat

OTHER:

- HTTP\_lua reduces the capture rate from >9G to <7G. At just under 5G this parser can be used in place of the native without dropping (in addition to the list above).
- xor\_executable pushes parse CPU to 100% and the system can drop significantly due to parse backup.

### **Aggregation Adjustments Based on Tested Live Content**

A 10G Decoder can serve aggregation to a single Concentrator while running at 10G speeds. Deployments using Malware Analysis, Event Stream Analysis, Warehouse Connector, and Reporting Engine are expected to impact performance and can lead to packet loss.

For the tested scenario, the Concentrator aggregates between 45 and 70k sessions/sec. The 10G Decoder captures between 40-and 50k sessions/sec. With the content identified above, this is about 1.5 to 2 million meta/sec. Due to the high volume of session rates, the following configuration changes are recommended:

- Nice aggregation on the Concentrator limits the performance impact on the 10G Decoder.  
The following command turns on nice aggregation.  
`/concentrator/config/aggregate.nice = true`

- Due to the high volume of sessions on the Concentrator, you may consider activating parallel values mode on the Concentrator by setting `/sdk/config/parallel.values` to 16. This improves Investigation performance when the number of sessions per second is greater than 30,000.
- If multiple aggregation streams are necessary, aggregating from the Concentrator instead has less impact on the Decoder.
- Further review for content and parsing is required for deployments where you want to use other NetWitness Suite components (Warehouse, Malware Analysis, ESA, and Reporting Engine).

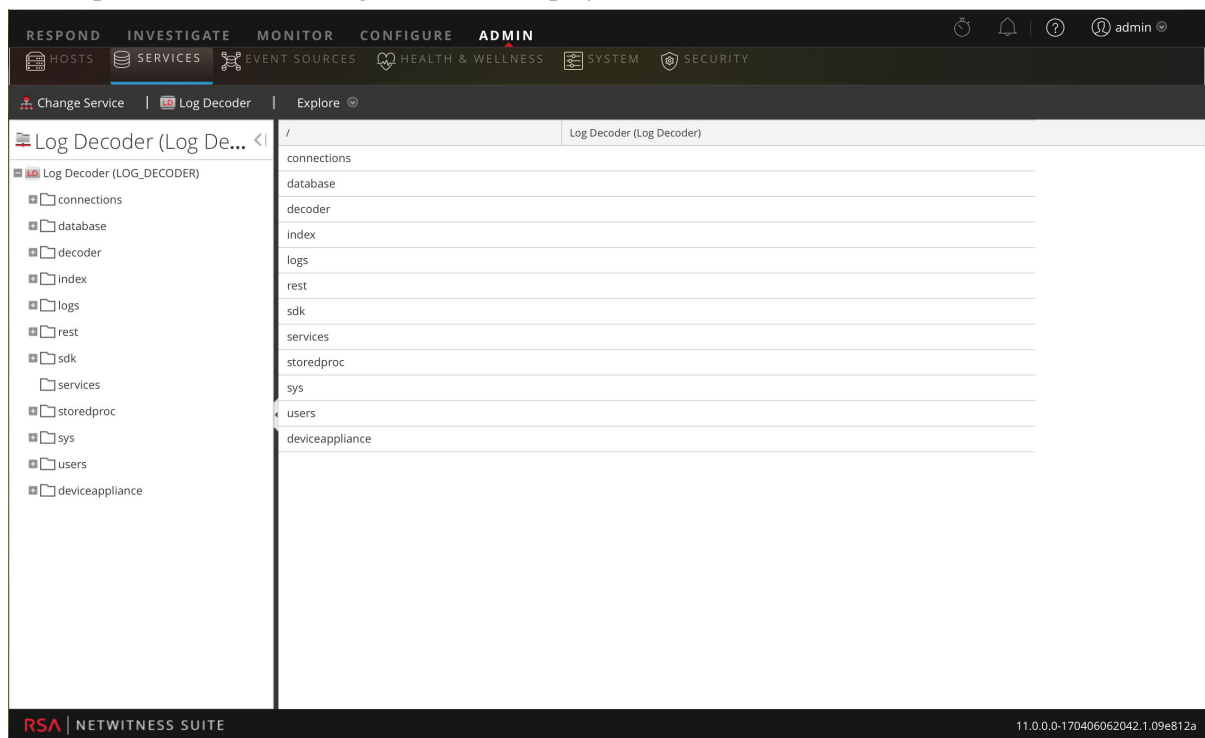
## Configure a Log Decoder to Accept Protobuf

There are occasions when you want to analyze log files that are in protobuf (Protocol Buffer) format. You can configure a Log Decoder to accept logs in protobuf (Protocol Buffer) format.

### To import a log file to a Log Decoder:

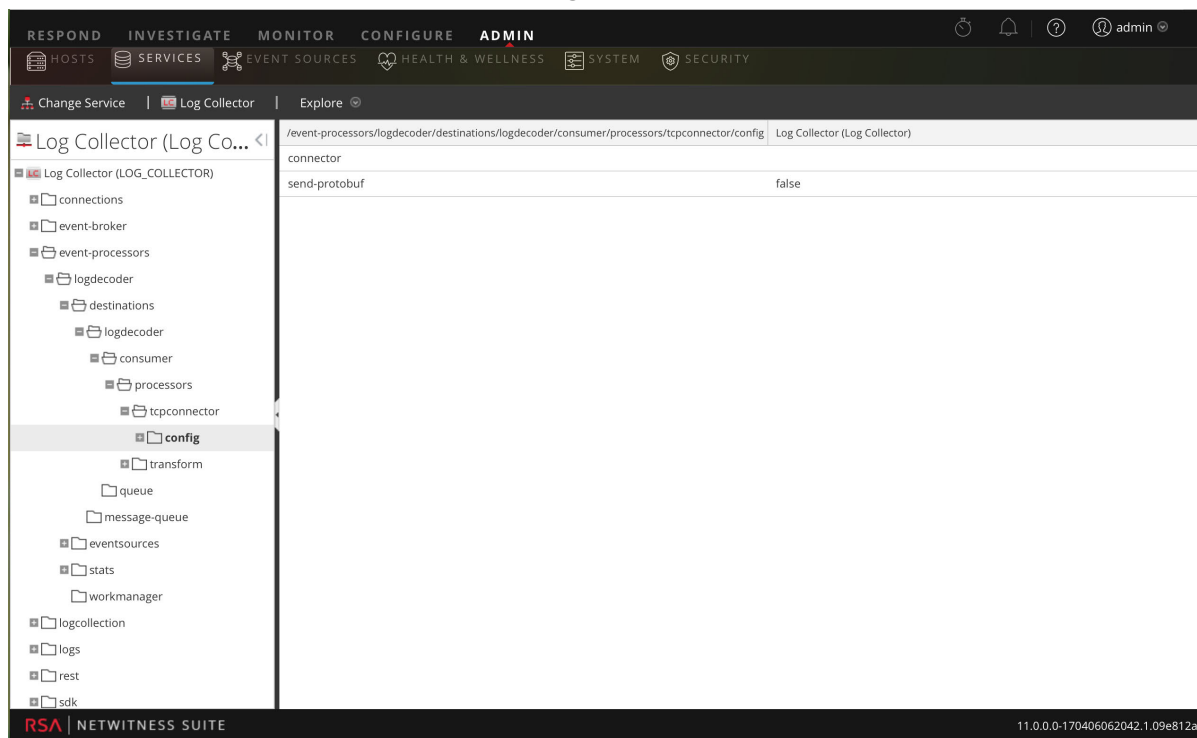
1. Go to **ADMIN > Services**.
2. Select a Log Decoder in the **Service** list, and select   > **View > Explore**.

The Explorer view for the Log Decoder is displayed.



3. Navigate to event-  
processors/logdecoder/destinations/logdecoder/consumer/processors/  
tcpconnector/config

Your screen should look similar to the following.



4. For the **send-protobuf** field, select **false**, and change the value to **true**.
5. Navigate to event-processors/logdecoder/destinations/logdecoder/consumer/processors/tcpconnector/config/connector/channel/tcp and change the **port** value to **50202**.
6. Navigate to event-processors/logdecoder/destinations/logdecoder/consumer/processors/tcpconnector/config/connector/event and change the following parameters:
  - Clear the **delimiter** field
  - Change **format** to **%text%**

## Configure Session Split Timeouts

The default behavior of the Decoder is to automatically end sessions that exceed a configured size or have been inactive for a period of time. When the session is ended due to timeout, any subsequent packets received in that session appear to be stored in a new session. You can mitigate the effect of session splitting due to long periods of inactivity between packets using this procedure.

When a Decoder session exceeds a configured size (32MB by default, the `/decoder/config/assembler.max.size`) or has been inactive for a period of time, the session is split. NetWitness Suite has the previous packet and the next packet and can propagate session state from the initial session fragment to the subsequent session fragment.

Each session fragment is annotated (`session.split` meta) such that it can be identified and associated with other fragments from the actual network session. Directionality as determined by the initial session reduces the occurrence of fragments having reversed directionality.

If there is a gap in time between packets large enough that there are no longer any packets for the session in memory, the session is removed from the Decoder. If a subsequent packet shows up after this occurs, a new session is created with no context to the preceding session. The issue is the inability to continue a session when we encounter a gap between packets of a session that is larger than the packets we are buffering (based upon available memory and timeout configurations). Once the last packet of a session is removed from memory, the session is also removed, and with it the necessary context for ensuring consistent directionality.

There are two timeout settings in a Packet Decoder, `/decoder/config/assembler.timeout.session` and `assembler.timeout.packet`. Both default to 60 seconds. The setting `assembler.timeout.session` controls how long a session lives in Assembler without receiving another packet. The setting `assembler.timeout.packet` controls how long a session waits before getting parsed. If the session is kicked out of Assembler before this timeout, then it automatically goes to parsing.

The session timeout is the number of seconds since the last packet was added to that session. Therefore, this timeout resets on every packet added to that session. The packet timeout is the number of seconds since the very first packet for that session was added (in other words, the packet that created the session). This is never reset and once the timeout expires, the session is parsed.

The important point is a session can be parsed but still remain in Assembler. A session in Assembler can still have packets added to it, even if it has already been parsed. Packets added after the session is parsed will never be seen by parsers, but they will be attached to the session and can be viewed by a subsequent `/sdk content` or `/sdk packets` call.

After a session is parsed, the session AND its metadata are written to disk. At this point, they can be aggregated and "seen" by `sdk` commands. Packets are written in order of capture and are not reordered by what session they belong to. Nor are they necessarily written when the session and meta data are written.


You can disable both timeout nodes, `/decoder/config/assembler.timeout.session` and `assembler.timeout.packet`, by setting them to zero in the Services Explore view.

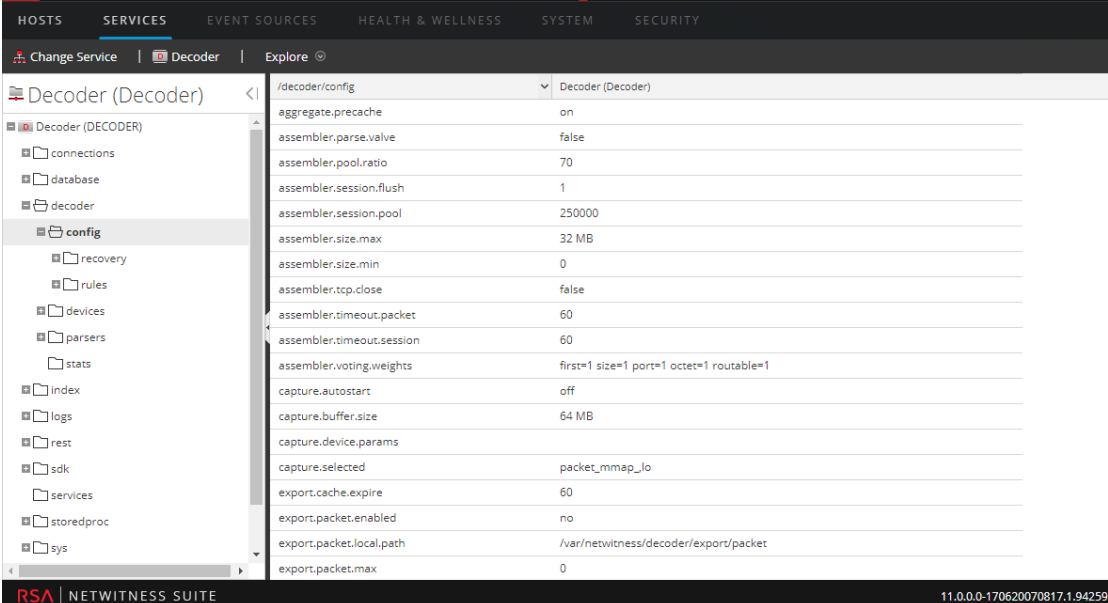
If both timeouts are disabled, the sessions are still split due to time or size expiration. However, the Decoder keeps track of the network stream for as long as it has sufficient memory. Thus, when more packets arrive on the same network stream, the Decoder adds `split` meta items to the subsequent sessions. Using a combination of the `split` metadata and the stream key, it is possible to reconstruct the network stream from the multiple sessions.

The length of time for which sessions are tracked is limited by the number of session pool entries available on the Decoder, and therefore the actual time window varies according to the rate at which new sessions are added. If new sessions are added at a high rate, the size of the time window decreases. The size of the pool is set using the configuration entry `/decoder/config/assembler.session.pool`, which sets the maximum number of sessions that will be tracked at a time.

The `/decoder/stats/assembler.timespan` statistic allows you to see when the Decoder is no longer tracking session splits because the ingest rate is too high and the Decoder does not have enough memory to track. This statistic shows the number of seconds tracked within the session table, which is the effective time window in which the Decoder can link together sessions. Under normal operation this statistic matches the value of `/decoder/config/assembler.timeout.session`, but when running in Time Split mode, the `/decoder/stats/assembler.timespan` statistic grows or shrinks depending on the ingest rate.

### To configure Time Split mode, set the following configuration parameters and restart the Decoder:

1. In the Admin > Services view, select the Decoder service and  > View > Explore.
2. In the Services Explore view select **decoder** > **config**.



The screenshot shows the RSA NetWitness Suite interface. The top navigation bar includes tabs for HOSTS, SERVICES, EVENT SOURCES, HEALTH & WELLNESS, SYSTEM, and SECURITY. The SERVICES tab is active, and the Decoder service is selected. The left sidebar shows a tree view of the Decoder service configuration, with 'config' selected. The main panel displays a list of configuration parameters for the Decoder service, including:

Parameter	Value
<code>/decoder/config/aggregate.precache</code>	on
<code>assembler.parse.valve</code>	false
<code>assembler.pool.ratio</code>	70
<code>assembler.session.flush</code>	1
<code>assembler.session.pool</code>	250000
<code>assembler.size.max</code>	32 MB
<code>assembler.size.min</code>	0
<code>assembler.tcp.close</code>	false
<code>assembler.timeout.packet</code>	60
<code>assembler.timeout.session</code>	60
<code>assembler.voting.weights</code>	first=1 size=1 port=1 octet=1 routable=1
<code>capture.autostart</code>	off
<code>capture.buffer.size</code>	64 MB
<code>capture.device.params</code>	
<code>capture.selected</code>	packet_mmap_lo
<code>export.cache.expire</code>	60
<code>export.packet.enabled</code>	no
<code>export.packet.local.path</code>	/var/netwitness/decoder/export/packet
<code>export.packet.max</code>	0

The bottom of the interface shows the RSA NetWitness Suite logo and the version number 11.0.0.0-170620070817.1.94259.

- Click in the **Value** column next to the parameter and set these two parameters :  
`/decoder/config/assembler.session.flush = 0`  
`/decoder/config/assembler.timeout.session = 0`
- To see when the Decoder is no longer tracking session splits because the ingest rate is too high and the Decoder does not have enough memory to track, view the  
`/decoder/stats/assembler.timespan` statistic, in the Services Explore view select **decoder > stats**.

The screenshot displays the RSA NetWitness Suite interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The left sidebar shows a tree view of services, with 'Decoder (Decoder)' selected. The main panel shows the 'stats' view for the 'Decoder (Decoder)' service. The table below lists various statistics and their values.

Path	Value
assembler.timespan	60
capture.appfilter.bytes	0
capture.avg.size	168
capture.device	packet_mmap_
capture.dropped	0
capture.dropped.percent	0
capture.dropped.percent.max	0
capture.filtered	0
capture.header.bytes	9078828
capture.interface	lo
capture.kept	118150
capture.netfilter.bytes	0
capture.packet.rate	141
capture.packet.rate.max	235
capture.payload.bytes	17688310
capture.processed.bytes	26767138
capture.rate	0
capture.rate.max	0
capture.received	118150
capture.status	started
capture.total.bytes	26767138
correlation.results.created	0



The bottom of the interface shows the RSA logo and 'NETWITNESS SUITE' on the left, and the version '11.0.0.0-170406062042.1.09e812a' on the right.

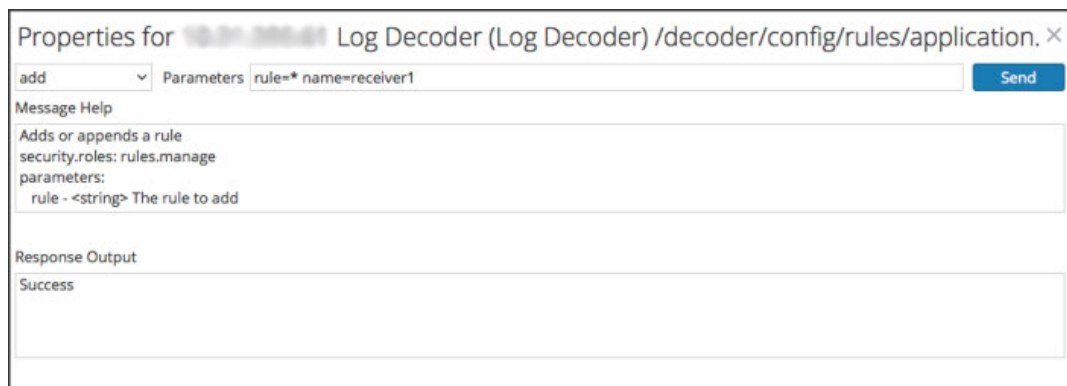
## Configure Syslog Forwarding to Destination

In addition to collecting Syslog messages, you can configure the Log Decoder to forward Syslog messages to another Syslog receiver. NetWitness Suite forwards Syslog messages after it has parsed the messages and before it writes the messages to the Log Decoder.

**Note:** You must configure Syslog Forwarding using the steps defined in this topic under **Procedure** using the **Explore** view.

The Log Decoder must be in the **Started** state before you can configure Syslog Forwarding. To configure Syslog Forwarding:

1. Configure Log Decoder application layer rules (Application rules) to tag Syslog messages with metadata that instructs NetWitness Suite to forward the messages:
  - a. In the **Services** view, select a Log Decoder, and in the Actions column, select   **> View > Explore**.
  - b. Go to the `/decoder/config/rules/application` node, right-click **application**, and click **Properties**.
  - c. In the **Properties** view, specify the **add** command with the following parameters:  
`rule=<query> name=<name>`  
 Example 1: `rule=*name=receiver1`  
 Example 2: `rule="device.type='winevent_nic'" name=receiver)`
  - d. Click **Send**.



NetWitness Suite creates the `name=receiver1 rule=* order=<n>` rule. NetWitness Suite inserts the order number (for example, `order=49`) based on when you set up the rule.

0049

`rule=* name=receiver1 order=49`





- e. Go to the `/decoder/config/rules/application` node and click the `name=receiver1 rule=* order=49 rule`.
- f. Add **alert forward** parameters to the rule parameters.

`rule=* name=receiver1 order=49 alert forward`

All other rule parameters have the same meaning as they do in other application rules.

The following Application rule example selects all logs with the `*` rule. It creates an alert meta with the value `"receiver1"` and tags the entire log for forwarding it to the syslog forwarding destination. You can define as many different forwarding rules as you need with the same name or unique names.

2. Define Syslog forwarding destinations and enable forwarding.
  - a. In the **Services** view, select a Log Decoder, and   > **View > Explore**.

- b. Syslog forwarding destinations are defined in the configuration node `/decoder/config/logs.forwarding.destination`.

This configuration node contains one or more name/value pairs. The name corresponds to the name parameter in the application rule that you used to tag logs with forwarding meta. The value is a colon-separated triple of transport, host, and port followed by an optional formatting parameter.

```
name=(udp|tcp|tls):host:port[:(retainsource|rfc3164)]
```

The first parameter indicates the transport protocol and must be one of `udp`, `tcp`, or `tls`. Specifying `udp` will forward logs via RFC 3164 / RFC 5426 UDP syslog protocol. Specifying `tcp` will forward logs via a TCP connection with RFC 6587 framing. Specifying `tls` will forward logs in accordance with RFC 5425.

The host is an IPv4 address, IPv6 address, or host name.

The port is the port to which the logs are sent. This is typically port 514 for UDP syslog, and 6514 for TLS connections. There is no standard port assignment for syslog over TCP.

Optionally, `retainsource` or `rfc3164` can be specified at the end of the destination string to indicate that additional formatting and information should be included with each log forwarded. Specifying `retainsource` will include z-connector headers at the beginning of the log based and will be populated by the time, device.(ip|ipv6|host), and `lc.cid` meta and is best used for forwarding to other log decoders. The `rfc3164` option will prepend a valid RFC3164 header to all events forwarded constructed of the `syslog.pri`, time, and device.(ip|ipv6|host) meta. In both cases, the original log text is unmodified.

Example forwarding destination:

```
gears=tls:gears.netwitness.local:6514
```

Example forwarding over tcp to blackout on port 514 with z-connector headers:

```
fwdrule=tcp:blackout.netwitness.local:514:retainsour
```

In the `/decoder/config/logs.forwarding.destination` parameter, specify the destination. For example:

TLS Connections: `receiver1=tls:receiver1.netwitness.local:6514`

UDP Connections: `receiver1=udp:receiver1.netwitness.local:514`

TCP Connections: **`receiver1=tcp:receiver1.netwitness.local:514`**

<code>logs.forwarding.destination</code>	<code>receiver1=tcp:10.31.244.44:514 receiver2=tcp:10.31.244.46:514 receiver3=tcp:10.31.244.48:514</code>
------------------------------------------	-----------------------------------------------------------------------------------------------------------

#### Note:

You can configure:

- Multiple rules to forward logs to the same destination.
- Multiple rules to forward logs to multiple destination.

For TLS connections, the certificate of the forwarding destination must be validated. The certificate authority that signed the destination's certificate must be present in the Log Decoder's CA trust store and the certificate must reside on the destination or Syslog receiver. Refer to "Configure Certificates" in the *Log Collection Configuration Guide* for information about manipulating the Log Decoder's CA trust store. (Go to the [Master Table of Contents](#) for Version 11.0 to find NetWitness Suite 11.0 documents.)

- c. In the `/decoder/config/logs.forwarding.enabled` parameter, specify **true**.

<code>logs.forwarding.enabled</code>	<b>true</b>
--------------------------------------	-------------

## Configure Transaction Handling on a Decoder

Beginning with 11.0, administrators can configure a Decoder to subdivide incoming sessions into smaller transaction sessions when using LUA parsers designed to create transactions. The feature allows analysts to perform analytics on the split sessions in downstream services such as Investigate.

### Transaction Handling

The Decoder service configuration node has a new parameter for configuration of transaction handling: `/decoder/parsers/config/parser.transaction.mode`. This node controls the behavior of the Decoder when a parser defines a transaction within a network session.

The values for `parser.transaction.mode` correspond to the operating modes:

- `{{off}}` (transactions off)
- `{{meta}}` (transactions represented as meta Items)
- `{{split}}` (transactions split sessions)

#### Transactions Off

When transactions mode is off, any application-level transactions created by parsers are ignored, and nothing is stored in the collection to represent the transaction.

#### Transactions Represented as Meta Items

In this mode of operation, when a parser generates an application-level transaction, a new meta item of type `{{trans}}` is added to the session in which the transaction occurred. The `{{trans}}` meta item contains a list of other meta items that constitute the transaction.

#### Transactions Split Sessions

In this mode of operation, when a parser generates an application-level transaction, the session is split. The session splitting is accomplished by:

1. A new session item is created.
2. Network meta items are copied from the parsed session into the new session.
3. Meta items marked in the transaction are moved from the original session to the new session.

The following meta items are duplicated into the split session from the session that was parsed:

- `time`
- `medium`

- eth.src
- eth.dst
- eth.type
- ip.proto
- ip.src
- ip.dst
- ipv6.src
- ipv6.dst
- ipv6.proto
- tcp.srcport
- tcp.dstport
- tcp.flags
- udp.srcport
- udp.dstport
- service
- udp.srcport
- udp.srcport
- tls.premaster

## Decrypt Incoming Packets

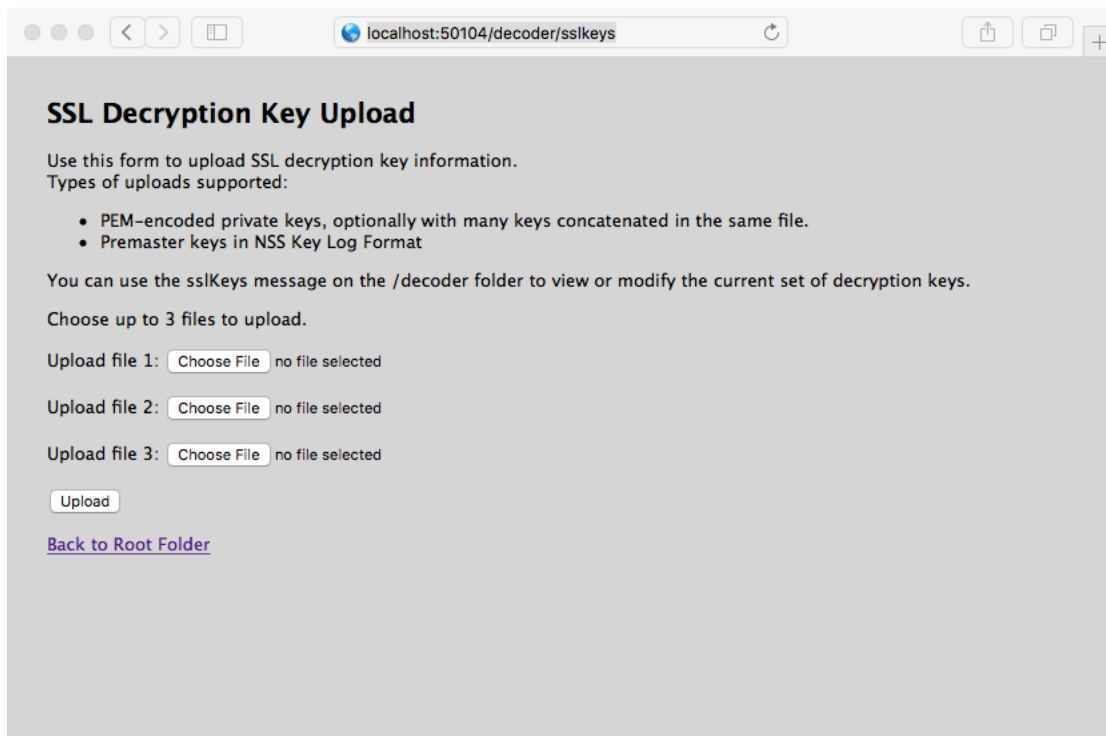
Beginning with NetWitness Suite 11.0, administrators can configure a Packet Decoder to decrypt incoming packets using the `sslKeys` command. Enabled parsers will see the unencrypted packet payload and create metadata accordingly. If the Decoder is not configured to decrypt incoming packets, most enabled parsers will see only encrypted garbage and will fail to create meaningful metadata.

**Note:** If FIPS is enabled, the list of ciphers for decryption is restricted to only those that are FIPS approved.

The `sslKeys` command provides a way to upload premaster or private keys to the Decoder, so that captured encrypted packets that match the keys can be decrypted before parsing. Administrators configure the Decoder by entering the `sslKeys` command using the NwConsole command line interface or the Decoder RESTful interface.

The screenshot shows the NetWitness Decoder RESTful interface. At the top, there's a navigation bar with links for 'SERVICES', 'storedproc (\*)', 'sys (\*)', and 'users (\*)'. Below this is a section titled 'Properties for /decoder' with a dropdown menu set to 'sslKeys' and a 'Send' button. A 'Message Help' section follows, containing detailed information about the `sslKeys` command, including its purpose (pushing SSL crypto information), security roles, and parameters like `clear`, `maxKeys`, and `random`. Below the help text is an 'Output (or command manual help)' section that provides instructions on how to generate premaster keys using a browser (Chrome or Firefox) and how to upload them to the Decoder using either a `login` command or a `curl` command. The `curl` command is shown as: `curl -u "<username>:<password>" -H "Content-Type: application/octet-stream" --data-binary @"/path/SSLKeys.txt" -X POST "http://<host>".` The page concludes with a section titled 'Private Keys or PEM files'.

The RESTful interface form at the path: `/decoder/sslkeys` allows uploading a single PEM-encoded private key, a single file containing multiple private keys concatenated together, or a single file of multiple premaster keys.



The screenshot shows a web browser window with the address bar displaying `localhost:50104/decoder/sslkeys`. The page title is "SSL Decryption Key Upload". Below the title, there is a brief instruction: "Use this form to upload SSL decryption key information. Types of uploads supported:". This is followed by a bulleted list: "• PEM-encoded private keys, optionally with many keys concatenated in the same file." and "• Premaster keys in NSS Key Log Format". A note states: "You can use the sslKeys message on the /decoder folder to view or modify the current set of decryption keys." Below this, it says "Choose up to 3 files to upload." There are three upload sections, each with a "Choose File" button and the text "no file selected". At the bottom of these sections is an "Upload" button. A link labeled "Back to Root Folder" is at the very bottom of the form.

Although the packets are decrypted during the parse stage, only the encrypted packets are written to disk. The matching premaster key used for decrypting is written to the `tls.premaster` meta key, which analysts can use to subsequently view unencrypted packets on demand.

Details for administrators to configure decryption of incoming packets, and for analysts to view unencrypted packets on demand are provided below.

## Performance Considerations

Decrypting packets in real time requires extra work in the parsing stage. Before implementing this feature, plan carefully to ensure the incoming traffic bandwidth does not overwhelm the available compute power. You may need more Decoders to decrypt traffic than you would need if not decrypting.

Packets captured on a Decoder normally have a timeout of ~60 seconds in the assembly stage before they are sent to the parsing step. If the Decoder is under memory pressure due to very high bandwidth, the lifetime of the packets in Assembler may be shortened. To alleviate this situation, you can configure a longer timeout value and increase the amount of memory available to hold packets in Assembly. Also, in order to perform decryption of the packets, the Decoder must receive the decryption key before the parsing stage.

**Note:** Currently, only TLS 1.2 and earlier protocols can be decrypted

With no feeds loaded, the following parsers enabled, and 50% of the sessions being decrypted, a Decoder can process traffic at 3 Gbps .

Parser Name	Description
SYSTEM	Session Details
NETWORK	Network Layer
ALERTS	Alerts
GeoIP	Geographic data based on ip.src and ip.dst
HTTP	Hyper Text Transport Protocol (HTTP)
HTTP_Lua	Hyper Text Transport Protocol (HTTP) Lua
FTP	File Transfer Protocol (FTP)
TELNET	TELNET Protocol
SMTP	Simple Mail Transport Protocol (SMTP)
POP3	Post Office Protocol (POP3)
NNTP	Network News Transport Protocol (NNTP)
DNS	Domain Name Service (DNS)
HTTPS	Secure Socket Layer (SSL) Protocol
MAIL	Standard E-Mail Format (RFC822)
VCARD	Extracts VCARD fullname and email information
PGP	Identifies PGP blocks within network traffic
SMIME	Identifies SMIME blocks within network traffic
SSH	Secure Shell (SSH)
TFTP	Trivial File Transfer Protocol (TFTP)
DHCP	Dynamic Host Configuration Protocol (DHCP and BOOTP)
NETBIOS	Extracts NETBIOS computer name information.
SNMP	Simple Network Management Protocol (SNMP)

Parser Name	Description
NFS	Network File System (NFS) protocol
RIP	Routing Information Protocol (RIP).
TDS	MSSQL and Sybase database protocol (TDS)
TNS	Oracle database protocol (TNS)
IRC	Internet Relay Chat (IRC) protocol
RTP	Real Time Protocol (RTP) for audio/video
SIP	Session Initiation Protocol (SIP)
H323	H.323 Teleconferencing protocol
SCCP	Cisco Skinny Client Control Protocol
GTalk	Google Talk (GTalk)
VlanGre	Vlan ID and GRE/EtherIP tunnel addresses
BITTORRENT	BitTorrent File Sharing Protocol
FIX	Financial Information eXchange Protocol
GNUTELLA	Gnutella file sharing protocol
IMAP	Internet Message Access Protocol
MSRPC	Microsoft Remote Procedure Call protocol
RDP	Remote Desktop Protocol
SHELL	Command Shell Identification
TLSv1	TLSv1
SearchEngines	A parser that extracts search terms
FeedParser	External Feed Parser

## Encryption Keys

The `sslKeys` command accepts two types of encryption keys:



- Premaster key: the symmetric key used in the TLS payload stream for encryption and decryption.
- Private key: the asymmetric private key used during the TLS handshake that encrypts the premaster.

### Premaster Key

The premaster key is generated randomly and is ephemeral for the life of one specific TLS session. Normally, there is not a good way to get premaster keys to a Decoder in time for the parsing step. However, both Chrome and Firefox can write the premaster keys they generate to a file. This is useful for testing purposes. To configure your browser to do this, create an environment variable called `SSLKEYLOGFILE` and assign it the pathname of a file to which the keys will be written. The Decoder will accept the file exactly as written and will use all the decryption keys in the file for any encrypted traffic it captures.

This is a sample NwConsole script that uploads the file to a Decoder:

```
login <decoder>:50004 <username> <password>
send /decoder sslKeys --file-data=SSLKeys.txt
```

This is an example using a curl command (with the RESTful port) to upload the file to a Decoder:

```
curl -u "<username>:<password>" -H "Content-Type: application/octet-stream" --data-binary
@"/path/SSLKeys.txt" -X POST "http://<hostname>:50104/decoder?msg=sslKeys"
```

After the symmetric keys are uploaded, they will immediately be used for any necessary decryption. Symmetric keys are stored in memory and there is a limit to how many can be stored at any point in time. As more keys are added, the earliest keys will be aged out. You can also add premaster keys by just passing the `random` and `premaster` parameters to `sslKeys`.

### Private Keys or PEM files

Private keys are normally stored in PEM files and are the asymmetric keys generated by services that accept TLS traffic. These keys are used during the TLS handshake to encrypt the premaster symmetric key that will be used for the rest of the payload encryption.

For example, if you have a web server whose traffic you want visibility into, you need to upload the private key it uses to encrypt traffic. You only need to do this once, as it is stored permanently (or until removed by a delete command). Private keys are automatically encrypted before storing to protect them. After upload, you must issue a parser reload command so that the newly installed key becomes visible to the HTTPS parser. Now, all TLS handshakes that use that private key will be able to be decrypted by the Decoder.

**Note:** Not all ciphers suites use a "known" private key (for example, Ephemeral Diffie Hellman). Encrypted traffic with those ciphers cannot be decrypted unless the premaster key is uploaded to the Decoder before the session is parsed.

These are some sample commands that upload a PEM file to be used for decryption.

Using NwConsole:

```
send /decoder sslKeys pemFilename=MyKey.pem --file-data=/path/MyKey.pem
```

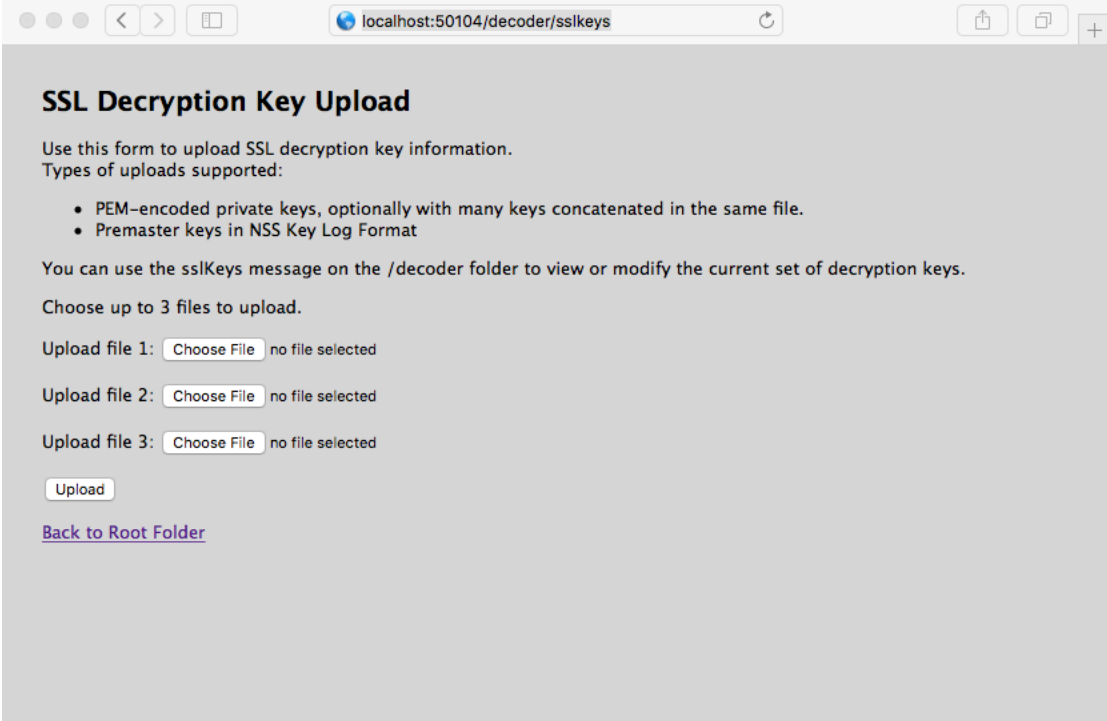
Using the RESTful interface (you must provide the `pemFilename` parameter in the URL):

```
curl -u "<username>:<password>" -H "Content-Type: application/octet-stream" --data-binary  
@"/path/MyKey.pem" -X POST  
"http://<hostname>:50104/decoder?msg=sslKeys&pemFilename=MyKey.pem"
```

## Upload Multiple Premaster and Private Keys

You can use the RESTful interface form to facilitate uploading of multiple keys, both premaster and private at the same time.

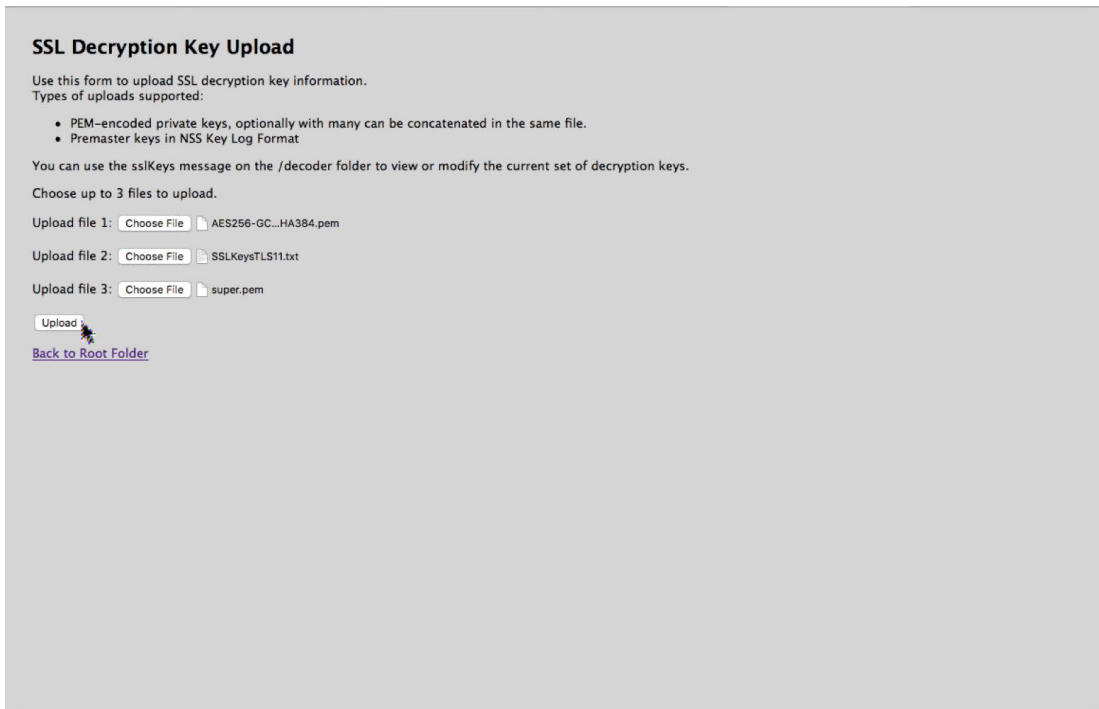
1. Open the RESTful API in your browser, and navigate to this path on the Decoder that you want to configure: `/decoder/sslkeys`.



The screenshot shows a web browser window with the address bar displaying `localhost:50104/decoder/sslkeys`. The page title is "SSL Decryption Key Upload". The main content area has a heading "SSL Decryption Key Upload" followed by the instruction "Use this form to upload SSL decryption key information. Types of uploads supported:". Below this, there is a bulleted list: "• PEM-encoded private keys, optionally with many keys concatenated in the same file." and "• Premaster keys in NSS Key Log Format". A paragraph follows: "You can use the sslKeys message on the /decoder folder to view or modify the current set of decryption keys." Below this is the instruction "Choose up to 3 files to upload." and three upload fields: "Upload file 1:", "Upload file 2:", and "Upload file 3:". Each field has a "Choose File" button and the text "no file selected". At the bottom of the form is an "Upload" button and a link labeled "Back to Root Folder".

2. Next to **Upload File 1**, click **Choose File** and locate the premaster key file or PEM file that you want to upload on you local file system.

3. (Optional) repeat for **Upload File 2** and **Upload File 3**.



**SSL Decryption Key Upload**

Use this form to upload SSL decryption key information.  
Types of uploads supported:

- PEM-encoded private keys, optionally with many can be concatenated in the same file.
- Premaster keys in NSS Key Log Format

You can use the sslKeys message on the /decoder folder to view or modify the current set of decryption keys.

Choose up to 3 files to upload.

Upload file 1:  AES256-GCM-HA384.pem

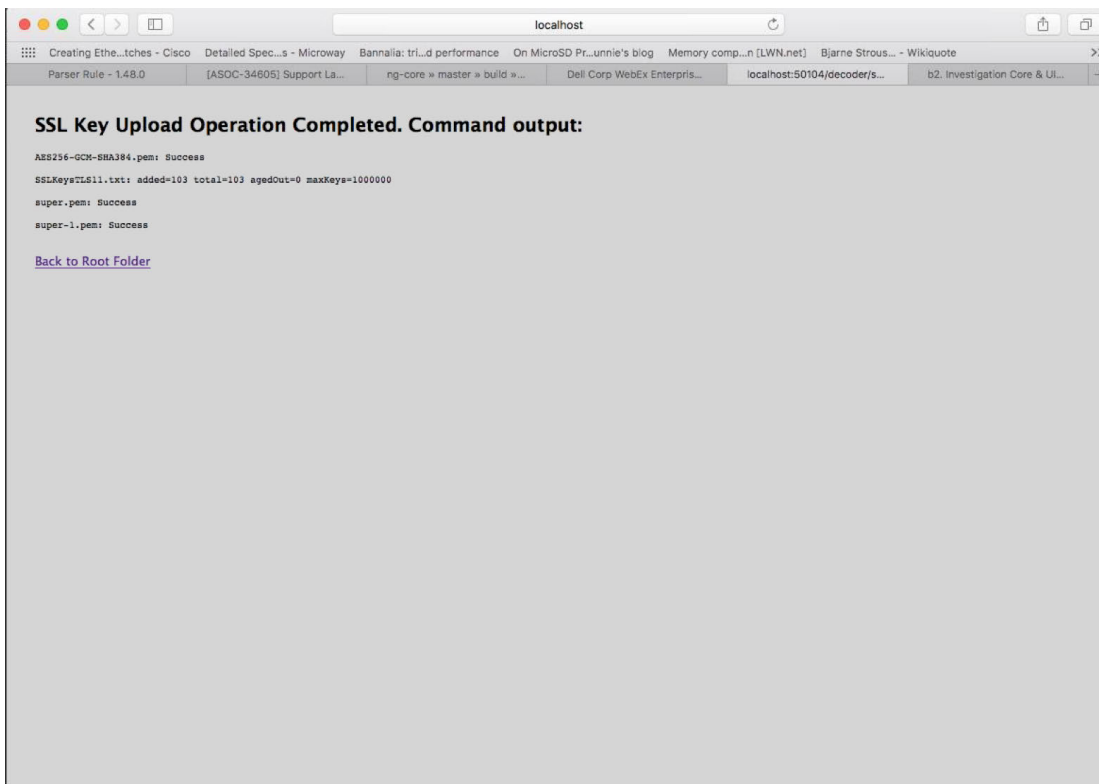
Upload file 2:  SSLKeysTLS11.txt

Upload file 3:  super.pem

[Back to Root Folder](#)

4. Click **Upload**.

The files are uploaded to the Decoder and results are displayed in the form.



**SSL Key Upload Operation Completed. Command output:**

```
AES256-GCM-SHA384.pem: Success
SSLKeysTLS11.txt: added=103 total=103 agedOut=0 maxKeys=1000000
super.pem: Success
super-1.pem: Success
```

[Back to Root Folder](#)

## Parameters for Managing Keys

The `sslKeys` command has several parameters for managing premaster and private keys. This is the full list of parameters:

Parameter	Description
<code>clear</code>	Removes all premaster keys from memory. Does not delete any PEM files installed on the system.
<code>maxKeys</code>	Changes the maximum number of premaster keys that are stored in memory.
<code>listPems</code>	Returns a list of all installed private key PEM files.
<code>deletePem</code>	Deletes the named PEM file from the file system. You can pass this parameter more than once to remove multiple files.
<code>random</code>	The random hash used to identify the premaster key.
<code>premaster</code>	The premaster key that will be installed for the previous <code>random</code> parameter. They must show up in pairs and <code>random</code> must be first.

## Return Values

Most `sslKeys` commands return name/value pairs of statistics about the premaster keys in memory. The statistics are listed in the following table.

Name	Description
<code>added</code>	The number of premaster keys just added during this command.
<code>total</code>	The total number of premaster keys loaded in memory.
<code>agedOut</code>	The total number of premaster keys that were removed during this command; this is not a lifetime stat.
<code>maxKeys</code>	The current maximum allowed premaster keys

## Viewing Unencrypted Traffic

If packets are decrypted during the parse stage, encrypted packets are written to disk, and the matching premaster key used for decrypting is written to the `tls.premaster` meta key, analysts can view the unencrypted packets using the `tls.premaster` meta key.

One Decoder API that you can use to see the unencrypted packets is the `/sdk/content` RESTful service. You need to know the Session ID of the encrypted packets and the `flags` parameter masked to the value 128 (or 0x80 in hex). Point your browser to the Decoder RESTful interface and type in the following command, substituting the actual Session ID for `<id>`:

```
http://<decoder>:50104/sdk/content&session=<id>&flags=128&render=text
```

The Decoder returns a simple web page showing the packets after they are decrypted.

If you want to see what the packets look like encrypted, type in one of the following commands, substituting the Session ID for `<id>`:

```
http://<decoder>:50104/sdk/content&session=<id>&render=text
```

```
http://<decoder>:50104/sdk/content&session=<id>&flags&render=text
```

For more information on the `/sdk/content` service, see the manual page for `/sdk content`.

## Edit Decoder System Configuration

When a service is first added to NetWitness Suite, default values for the system configuration parameters are in effect. In most cases, the default values for compression, statistics update interval, and number of threads in the thread pool are set at a good point for optimal system performance. You do not need to edit these setting unless an RSA Customer Support technician advises you to change them.

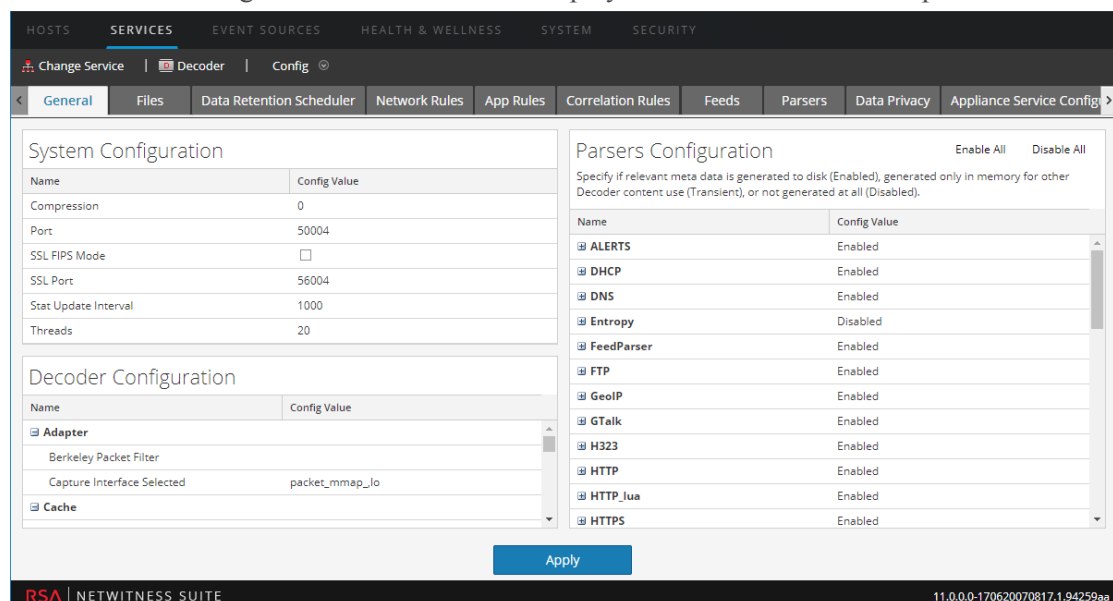
System Configuration	
Name	Config Value
Compression	0
Port	50004
SSL FIPS Mode	<input type="checkbox"/>
SSL Port	56004
Stat Update Interval	1000
Threads	20

One parameter that you may want to change for your environment is the SSL setting, which by default is not enabled. When enabled, the security of data transmission is managed by encrypting information and providing authentication with SSL certificates.

### To edit system configuration parameters for a Decoder or Log Decoder:

1. Go to **ADMIN > Services**.
2. In the Admin > System view, select a Decoder or Log Decoder service, and select   **> View > Config**.

The Services Config view for the service is displayed with the General tab open.



The screenshot displays the NetWitness Suite configuration interface for a service. The top navigation bar includes tabs for HOSTS, SERVICES, EVENT SOURCES, HEALTH & WELLNESS, SYSTEM, and SECURITY. The 'SERVICES' tab is active, and the 'Config' sub-tab is selected. Below the navigation bar, there are several tabs: General, Files, Data Retention Scheduler, Network Rules, App Rules, Correlation Rules, Feeds, Parsers, Data Privacy, and Appliance Service Config. The 'General' tab is currently open, showing two main configuration sections: 'System Configuration' and 'Decoder Configuration'. The 'System Configuration' section contains a table with the following data:

Name	Config Value
Compression	0
Port	50004
SSL FIPS Mode	<input type="checkbox"/>
SSL Port	56004
Stat Update Interval	1000
Threads	20

The 'Decoder Configuration' section also contains a table:

Name	Config Value
Adapter	Berkeley Packet Filter
Capture Interface Selected	packet_mmap_io
Cache	

To the right of these sections is the 'Parsers Configuration' section, which includes a table of parsers and their status. The status can be toggled between 'Enabled' and 'Disabled'.

Name	Config Value
ALERTS	Enabled
DHCP	Enabled
DNS	Enabled
Entropy	Disabled
FeedParser	Enabled
FTP	Enabled
GeoIP	Enabled
GTalk	Enabled
H323	Enabled
HTTP	Enabled
HTTP_lua	Enabled
HTTPS	Enabled

An 'Apply' button is located at the bottom center of the configuration area. The footer of the interface shows the RSA logo and 'NETWITNESS SUITE' on the left, and the version number '11.0.0.0-170620070817.1.94259aa' on the right.

3. Under **System Configuration**, click in a field that you want to edit (**Compression**, **Port**, **SSL FIPS Mode**, **SSL Port**, **Stat Update Intervals**, or **Threads**). Type a new value.
4. When finished editing, click **Apply**.  
The settings become effective immediately.

## Enable CPU Usage Statistics for Installed Content

Beginning with NetWitness Suite 11.0, the Decoder provides CPU utilization statistics for all installed content, which you can use to reveal how much CPU time is used by parsers, feeds, application rules, and lexical scanning. The statistics are visible as Stat nodes in the service tree from the Explorer view when **/decoder/parsers/config/detailed.stats** is enabled and the Decoder is capturing the stats.

Each piece of content is accounted as a single percentage value (0-100) regardless of the number of parse threads running. The percentage represents an average of the CPU utilization for the content across all threads.

To enable usage statistics monitoring:

1. Navigate to the Decoder Explorer view and select the `/decoder/parsers/config/detailed.stats` parameter.
2. Change the value to **enabled**. If the Decoder is not capturing data, start capture.  
When you open the Decoder Stats node in the Explorer view, the new statistic is visible.



## Enable Parser Mappings

This topic tells administrators how to enable event source mapping on a Log Decoder.

The Log Collector discovers the event source type on a per-message basis. If the correct parser is not identified for the event source, a small percentage of logs may be misidentified. The misclassified messages do not populate event source rules and alerts, and the reports do not have the correct data. If there are multiple event source types associated with an IP address, it makes it difficult for the parsers to identify the exact event source from which the logs are generated.


If you map an IP address to its event source type, the Log Decoder can identify the event source from which the log is generated. When messages are delivered to the Log Decoder from a mapped event source, only the assigned parsers are queried to find event matches.

You can assign event source types to IPV4, IPV6, or the hostname value of the event source. You can also assign multiple event source types to a single IP address. You can also use the Log Collector ID when different event source types with the same IP address are sent to different Log Collectors.

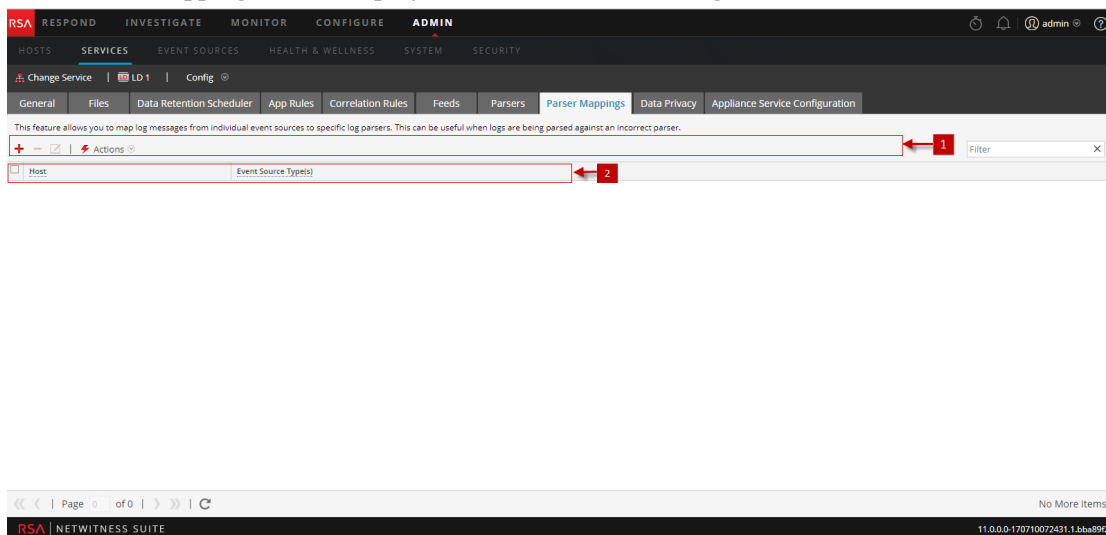
**Note:** You can also enable parser mapping functions by navigating to **ADMIN > Event Sources > Discovery**.

## Enable IP Address to Event Source Mapping

To enable an IP address to event source mapping:



1. Go to **ADMIN > System > Log Parser Mappings**.
2. Select **Decoder**, then select  > **View > Config**.
3. In the Configuration page, select the **Parser Mappings** tab.

The Parser Mappings tab is displayed in the Services Config view.

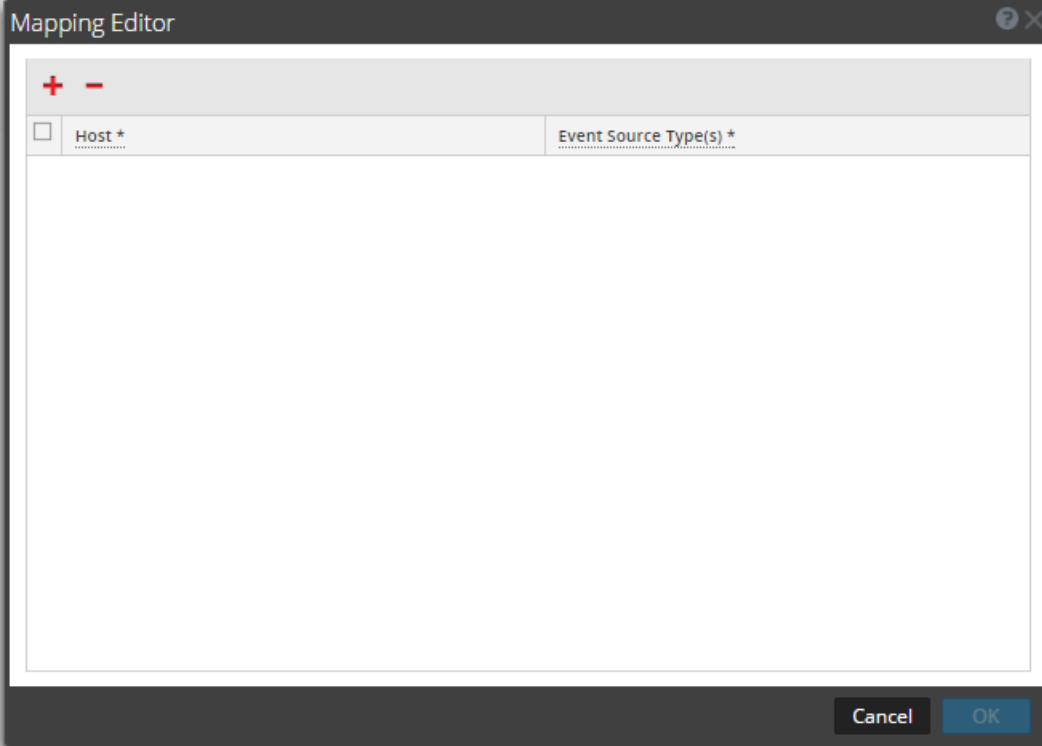


## Update IP to Event Source Mapping

To update an IP to event source mapping:

1. Go to **ADMIN > Services**.
2. Select a **Log Decoder**, and in the **Actions** column, select  > **View > Config**.  
The Services Config view is displayed.
3. Select the **Parsers Mapping** tab.
4. Click  .

The Mapping Editor is displayed.



The Mapping Editor dialog box is shown. It has a title bar with a question mark and a close button. Below the title bar is a header with a red plus icon and a minus icon. The main area is a table with two columns: 'Host \*' and 'Event Source Type(s) \*'. The 'Host \*' column has a checkbox to its left. The table is currently empty. At the bottom right are 'Cancel' and 'OK' buttons.

<input type="checkbox"/>	Host *	Event Source Type(s) *
--------------------------	--------	------------------------

5. Any of the following mappings can be defined:

### One Host and One Event Source Type

- In the **Host** field, enter the hostname.  
For example: 10.0.0.1
- In the **Event Sources(s)** field, enter the event source type.  
For example: apache

### One Host and One or More Event Source Types

- In the **Host** field, enter the hostname.  
For example: 10.0.0.1
- In the **Event Source(s)** field, enter the event source type.  
For example: apache, sap, aix

### One Host, One Log Collector, and One Event Source Type

- In the **Host** field, enter the hostname and Log Collector ID.  
For example: 10.0.0.1, LC-1.
- In the **Event Source(s)** field, enter the event source type.  
For example: apache

### One Host, One Log Collector ID, and One or More Event Source Types


- In the **Host** field, enter the hostname and Log Collector ID.  
For example: 10.0.0.1, LC-1
- In the **Event Source(s)** field, enter the event source type.  
For example: apache, sap, aix

**Note:** The event source types are processed in the order you enter the parsers and if one or more parsers matches a log, the first parser in the list is queried. The Host/IP can be IPv4, IPv6, or Hostname.

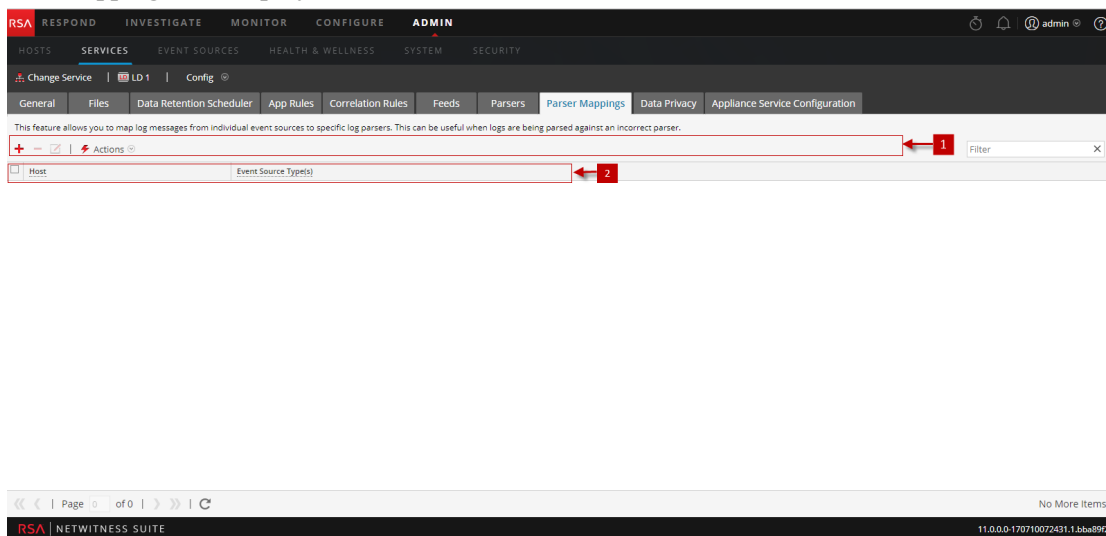
6. Click **OK**.  
The Parser Mapping is added.
7. To cancel the parser mappings selection, click **Cancel**.

## Read IP to Event Source Type Mappings

To read an IP to event source type mappings:



1. Go to **ADMIN > Services**, and select a Log Decoder service.
2. In the Actions column, select  > **View > Config**.  
The Services Config view is displayed.

3. Select the **Parsers Mapping** tab.  
The mappings are displayed.





## Edit an IP to Event Source Type Mapping

To edit an IP to event source type mapping:

1. Go to **ADMIN > Services**, and select a Log Decoder service.
2. In the Actions column, select  > **View > Config**.  
The Service Config view is displayed.
3. Select the **Parser Mappings** tab.
4. Select the mapping you want to edit.  
**Note:** You can only edit one mapping at a time.
5. Click .
6. In the **Event Source(s)** field, modify the event source(s).  
**Note:** The host is not editable and the field is disabled.
7. Click **OK** to accept the edited Event Source.
8. To cancel the changes, click **Cancel**.


## Delete an IP to Event Source Type Mapping

To delete an IP to event source type mapping:

1. Go to **ADMIN > Services**, and select a Log Decoder service.
2. In the Actions column, select  > **View > Config**.  
The Service Config view is displayed.
3. Select the **Parser Mappings** tab.
4. Select the mapping you want to delete.
5. Click .
- The mapping is deleted and the grid is refreshed.
6. To cancel the changes, click **Cancel**.

## Sort the Hostname or Event Source Type



To sort the hostname or event source type:

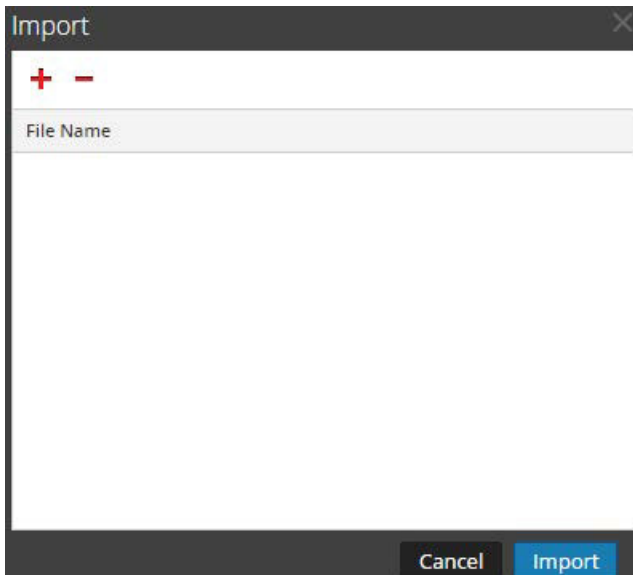
1. Go to **ADMIN > Services**, and select a Log Decoder service.
2. In the Actions column, select  > **View > Config**.  
The Service Config view is displayed.


3. Select the **Parser Mappings** tab.
4. To sort a column, click in the column header.  
Event Source Type(s) are applied for your selected IP address. Logs are parsed against the parsers in the order they are listed.

## Import IP to Event Source Mapping Entries

To import IP to event source mapping entries:

1. Go to **ADMIN > Services**, and select a Log Decoder service.
2. In the Actions column, select   > **View > Config**.  
The Service Config view is displayed.
3. Select the **Parser Mappings** tab.
4. Select **Actions > Import**.  
The Import dialog is displayed.




5. Click  .
6. Select the file you want to import and click **OK**.
7. To load the parser, click **Import**.

**Note:** You can only import one .csv file at a time.

## Export IP to Event Source Mapping Entries

To export IP to event source mapping entries:

1. Go to **ADMIN > Services**, and select a Log Decoder service.
2. In the Actions column, select  > **View > Config**.  
The Service Config view is displayed.
3. Select the **Parser Mappings** tab.
4. Select the mappings you want to export.
5. Select **Actions > Export > Selection**.


The Export Selection dialog is displayed.

A screenshot of the 'Export Selection' dialog box. It has a dark gray header with the title 'Export Selection' and a close button (X). Below the header is a light gray input field with the placeholder text 'Enter File Name'. At the bottom of the dialog are two buttons: 'Cancel' and 'Export'.

6. Enter the file name and click **Export**.

## Search IP to Event Source Mapping Entries

To search IP to event source mapping entries:

1. Go to **ADMIN > Services**, and select a Log Decoder service.
2. In the Actions column, select  > **View > Config**.  
The Service Config view is displayed.
3. Select the **Parser Mappings** tab.
4. In the Parsers Mappings toolbar, enter the Host or Event Source in the **Filter** field.
5. Click **Enter**.  
The Hosts or Event Sources that match the names entered in the **Filter** field are displayed.

## Enable or Disable Lua and Flex Parsing Systems



This topic tells administrators how to enable or disable Lua and Flex parsing systems on a Decoder or Log Decoder. Flex parsers are deprecated and disabled by default.

The settings to enable or disable Lua and Flex parsing systems are configured correctly by default and you do not typically have to change them. However, you may need to adjust these settings at the request of RSA Customer Care or for troubleshooting purposes.

In addition to configuring individual parsers, you can enable and disable all Lua parsing as well as all Flex parsing in the Services Explore view. You enable and disable the Lua parsing and Flex parsing systems settings separately, but they work in the same way.

- If you **disable** the Lua or Flex parsing system, the corresponding parsing system is disabled and no parsers are loaded.
- If you **enable** the Lua or Flex parsing system, the corresponding parsing system is enabled and individual parsers are enabled and disabled following the current individual configurations.

### To enable or disable Lua and Flex parsing systems on a Decoder or Log Decoder:

1. Go to **ADMIN > Services**.
2. Select a Decoder or Log Decoder and   > **View > Explore**.  
The Services Explore view for the selected service is displayed.
3. In the Node list, navigate to and select **/decoder/parsers/config**.
4. In the Monitor panel:
  - To enable the Lua parsing system, in the value field for `lua.enabled`, type **yes**.
  - To disable the Lua parsing system, in the value field for `lua.enabled`, type **no**.
  - To enable the Flex parsing system, in the value field for `flex.enabled`, type **yes**.
  - To disable the Flex parsing system, in the value field for `flex.enabled`, type **no**.

## Map IP Address to Service Type for Log Parsing

This topic describes the procedure to map an IP address to a service type for log parsing.



The Log Collector discovers event source type on a per-message basis. If the correct parser is not used for the specific event source, the messages that are common between event source types are misclassified. The misidentified messages will not populate service rules and alerts, and the reports will not have proper information. Also, if there are multiple services associated with an IP address, it can be difficult for the parsers to identify the exact service from which the log is generated.

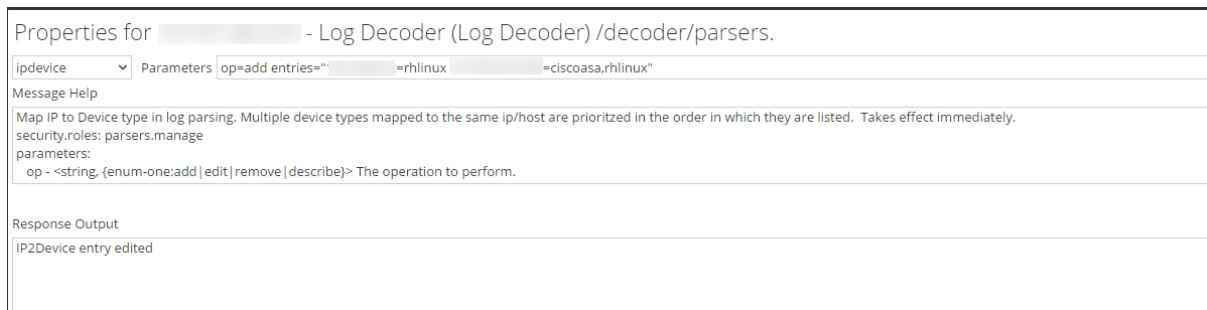
If you map an IP address to its services, the log decoder can identify the service from which the log is generated. When messages come into the log decoder from a mapped service, the assigned parsers are loaded to find event matches.

You can assign service types to IPV4, IPV6 or hostname value of the event source. You can also assign multiple service types to a single IP address. You can also use the CollectorID when different service types with the same IP address are sent to different collectors.

### Map an IP Address to a Service Type

To map an IP address to a service type, do the following:

1. Go to **ADMIN > Services**.
2. In the **Services** view, select a Log Decoder, and in the **Actions** column, select   > **View > Explore**.
3. Go to **/decoder/parsers** node, right-click **parsers**, and select **Properties**.
4. In the **Properties** view, specify the **ipdevice** command with the following parameters:  
`op=add/remove entries="ipaddress=service" (for example, op=add entries="10.100.201.300=ciscoasa")`
5. Click **Send**.



Properties for [redacted] - Log Decoder (Log Decoder) /decoder/parsers.

ipdevice ▼ Parameters op=add entries=" [text input: '=rhlinux'] [text input: '=ciscoasa,rhlinux']

Message Help

Map IP to Device type in log parsing. Multiple device types mapped to the same ip/host are prioritized in the order in which they are listed. Takes effect immediately.

security.roles: parsers.manage

parameters:

op - <string, {enum-one:add|edit|remove|describe}> The operation to perform.

Response Output

IP2Device entry edited

### IPdevice Command

In the `ipdevice` command, three operations are available:



- **add:** This operation adds or updates entries in the ipdevice map. Multiple space delimited address/type pairs may be specified.  
`op=add entries="<address>=<service type>"`
- **remove:** This operation removes entries from the ipdevice map. Multiple space delimited address/type pairs may be specified.  
`op=remove entries="<address>"`
- **describe:** This operation returns the values currently in the ipdevice map.

## Map an IP Address to a Time Zone



Often times logs do not fully specify timestamps and may be missing time zone information. To properly normalize such timestamps to UTC, the Log Decoder provides the ability to associate devices from a specific address (IPv4 or IPv6) or hostname to a time zone or a fixed offset.

Three time zone formats are currently accepted and are shown in the following examples:

- Olson format: America/Anguilla
- POSIX format: AST2:45ADT0:45,M4.1.6/1:45,M10.5.6/2:45
- Offset by Hours format: = -500

NetWitness Suite maps the device address (IPv4 or IPv6) or hostname to a specific time zone or offset. Event time meta that is parsed from a log that is from a mapped address and does not include an offset or time zone as part of the timestamp is adjusted to UTC according to the mapping.

### To map an IP address to a time zone, do the following:

1. Go to **ADMIN > Services**.
2. In the **Services** view, select a Log Decoder, and in the **Actions** column, select   > **View > Explore**.
3. Go to **/decoder/parsers** node, right click **Parsers**, and select **Properties**.
4. In the **Properties** view, specify the `iptmzone` command with the following parameters:  
`op=add entries="ipaddress=timezone"` (for example, `op=add entries="10.10.10.10=Africa/Addis Ababa"`)
5. Click **Send**.

### iptmzone Command

In the `iptmzone` command, three operations are available:

- **add:** This operation adds or updates entries in the iptmzone map. Multiple space delimited address/type pairs may be specified.  
`op=add entries="<address>=<time zone>"`
- **remove:** This operation removes entries in the iptmzone map. Multiple space delimited address/type pairs may be specified.  
`op=remove entries="<address>"`
- **describe:** This operation returns the values currently in the iptmzone map.

### Examples

The following examples provide instances for mapping IP addresses to time zones:

- If you want to map two different entries with different IPV4 values and time zone, enter the following parameter in the **iptmzone** command and click **Send**  
`"op=add entries="10.10.10.10=America/Anguilla  
10.10.10.11=Pacific/Rarotonga"`
- If you want to remove an entry for a single IPV4 value and time zone, enter the following parameter in the **iptmzone** command and click **Send**.

```
"op=remove entries=10.5.245.9"
```

- If you want to create a single entry for an IPV6 value and time zone, enter the following parameter in the **iptmzone** command and click **Send**.

```
op=add entries="2001:DB8:85A3::8A2E:370:7334=America/Anguilla"
```


- If you want to create a single entry to map an IPV4, IPV6, or hostname with the Minute Offset, Olson, or POSIX format, enter the following parameter in the **iptmzone** command and click **Send**.

```
op=add entries="10.168.0.2=America/Anguilla  
2001:DB8:85A3::8A2E:370:7334=0500nwappliance21=EST5EDT,M3.2.0/2  
,M11.1.0"
```

## Obtain Log Files a from Pre-11.0 Log Decoder

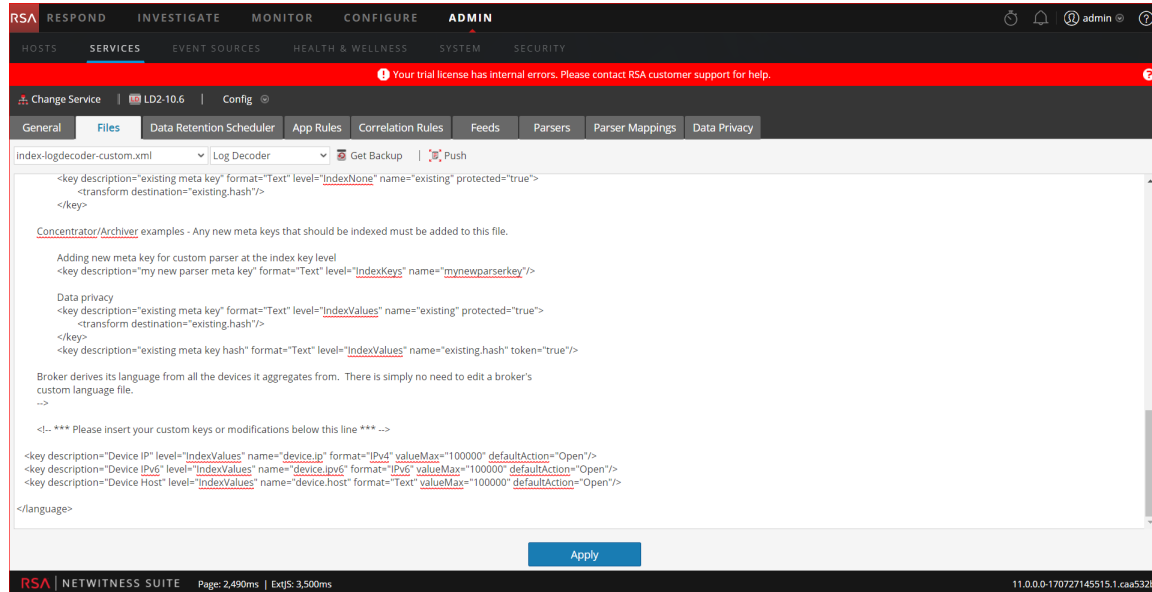
NetWitness 11.0. added the capability to view a small sampling of recent logs for specific devices through detail tabs of the Discovery View. By default, Log Decoders prior to 11.0 do not have the necessary configuration to enable this feature, but a few minor changes can make it available.

To enable logs preview for a pre-11.0 Log Decoder, follow these steps on the Log Decoder:

1. Go to **ADMIN > Services >** select a **Log Decoder**, then select  **> View > Config**.
2. Click the **Files** tab and select **index-logdecoder-custom.xml** from the drop-down menu.
3. Add the following three lines at the end of the file (before the closing language tag):
 

```
<key description="Device IP" level="IndexValues" name="device.ip" format="IPv4"
valueMax="100000" defaultAction="Open"/>
<key description="Device IPv6" level="IndexValues" name="device.ipv6" format="IPv6"
valueMax="100000" defaultAction="Open"/>
<key description="Device Host" level="IndexValues" name="device.host" format="Text"
valueMax="100000" defaultAction="Open"/>
```
4. Click **Apply**.
5. Restart the Log Decoder service as follows.  
Select Log Decoder service > **Explore > decoder > Properties > reset**

This is an example of the **index-logdecoder-custom.xml** file.



**Note:** Discovery Scores are only available for 11.x and above Log Decoders. Discovery Scores for pre-11.x Log Decoders are displayed as Unavailable.

The following example shows the Discovery Score as **Unavailable** in the **Details** view for a pre-11.0 Log Decoder.

Event Source	Discovery Score	Acknowledged	Mapped	Log Collector(s)	Log Decoder(s)	Event Source Type(s)
sa11ld206	Unavailable	No	No	sa11vic206	logdecoder	unknown
LD-2	Unavailable	No	No	LC4	logdecoder	bigfix
2001::	Unavailable	No	No	LC6	logdecoder	bigfix
LD2	Unavailable	No	No	LC2	logdecoder	bigfix

**Note:** Device logs are only available for 11.x and above Log Decoders.

The following example shows the message that is displayed in the Logs panel for a pre-11.0 Log Decoder.

Event Source Type	Discovery Score
bigfix	Unavailable

Timestamp	Log Decoder	Discovery Score	Message
-	10.31.204.85	-	Discovery logs view is only available for 11.x and above Log Decoders by default. See documentation (link?) for enabling on earlier versions.

Attributes	
Log Collector	3522f8a0416c469c96e0b879af4ad664
UPS Protected	false

## Upload a Log File to a Log Decoder



This topic describes the method for importing a log file to a Log Decoder.

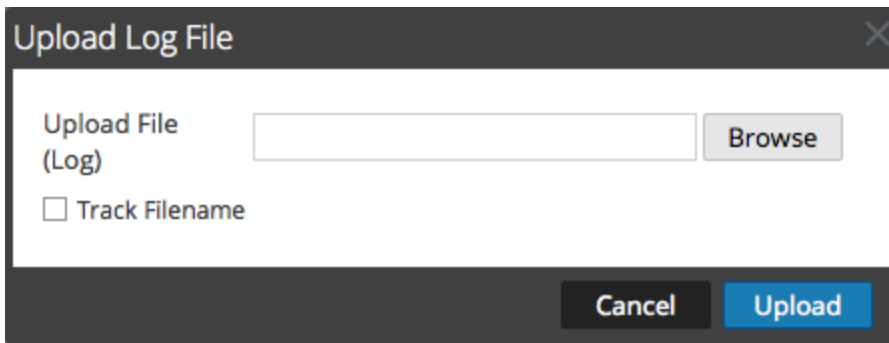
There are occasions when you want to analyze a log file that is not available on the service you are using. You can upload a log file captured on another service to NetWitness Suite. Log filenames are of the type **.log**.

When a log file is uploaded to a Log Decoder, the Log Decoder analyzes and generates meta for each log it contains. These logs are added to the already decoded logs on the Log Decoder and are available for analysis. NetWitness Suite includes a filename tracking option that makes searching for a particular set of logs easier. When the log file is uploaded with file tracking, the Log Decoder adds meta to each log based on the uploaded filename. You can then filter sessions for analysis using that meta.

The option to upload a log file is dimmed when other Log Decoder operations prevent an upload from occurring. For example, when the Log Decoder is capturing logs.

### To import a log file to an Log Decoder:

1. Go to **ADMIN > Services**.
2. Select a Log Decoder in the **Service** grid, and select   > **View > System**.  
The Services System view for the Log Decoder is displayed.
3. In the toolbar, click **Upload Log File**.



4. To choose a log file, click **Browse**.  
A directory view is displayed.
5. Select the log file that you want to upload.  
The filename is displayed in the **Upload File** field.
6. If you want the Log Decoder to add meta to the logs based on the filename, click the checkbox next to **Track Filename**.

7. To upload the file, click **Upload**.

The selected file is uploaded and a status message indicates that the file is uploaded. The log file is available for analysis.

## Upload a Packet Capture File

There are occasions when you want to analyze a packet capture file that is not available on the service you are using. You can upload a file captured on another service to NetWitness Suite. Supported packet capture file types are `pcap` and `pcap.gz`.

When a packet capture file is uploaded to a Decoder, the Decoder creates sessions from the packet capture file packets. These sessions are added to the already decoded sessions on the Decoder and are available for analysis. NetWitness Suite includes a filename tracking option that makes searching for a particular set of sessions easier. When the packet capture file is uploaded with file tracking, the Decoder adds meta to the sessions based on the uploaded filename. You can then filter sessions for analysis using that meta.

The option to upload a packet capture file is dimmed when other Decoder operations prevent an upload from occurring; for example, when the Decoder is capturing packets.

### To select and upload a packet capture file:

1. Go to **ADMIN > Services**.

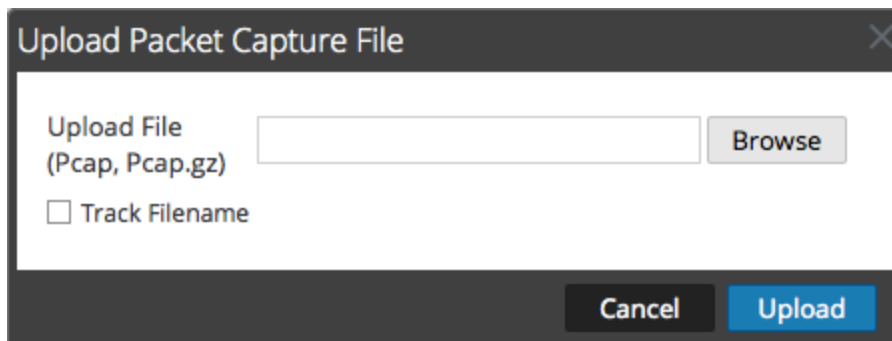
The Administration Services view is displayed.

2. Select the Decoder name, and   > **View > System**.

The Services System view for the Decoder is displayed.

3. In the toolbar, click **Upload Packet Capture File**.

The **Upload Packet Capture File** dialog is displayed.



4. To choose a capture file, click **Select**.

A directory view is displayed.

5. Browse the directory and select the packet capture file that you want to upload.

The filename is displayed in the **Upload File(pcap,pcap.gz)** field.

6. If you want the Decoder to add meta to the sessions based on the filename, click the checkbox next to **Track Filename**.

7. To upload the file, click **Upload**.

A progress bar shows upload progress.

Upload time varies depending on the size of the file. When the file upload is complete, a status message is displayed. The file is now available for investigation.



## Feed and Parser References

---

This topic provides more details about the feeds and parsers that the Decoder uses.

- [Feed Definitions File](#)
- [Flex Parsers](#)
- [Geo IP Parser](#)
- [Lua Parsers](#)
- [Search Parser](#)
- [Wireless LAN Configuration](#)

## Feed Definitions File

This topic introduces the feed definitions file, which is available for editing in the Services Config view > Files tab.

One of the files available for editing in the Services Config view > Files tab is **feed-definitions.xml**, the feed definitions file.

### **feed-definitions.xml**

You can define feeds in the `feed-definitions.xml` file. The Decoder uses an XML schema to define feed messages when it creates a binary `.feed` file from the feeds defined here.

For details on the feed definition language, refer to the NextGen System Administrator Guide.

## Flex Parsers

One of the files available for editing in the Services Config view > Files tab is **NwFlex.xml**, the flex parser.

### NwFlex.xml

There are two kinds of Flex parsers:

- **Service identification based solely on port.** These are parsers that use only the source or destination ports to identify the session application type (service). These are the most basic and easiest to define.
- **Service identification based on a found token(s).** These parsers use tokens to identify the service type. This is also an easy way to expand which service types are identified. These are important when identifying non -internet standard applications. These parsers require that the protocol has a definable token that can uniquely identify the service type.

Five common parser operations are:

- Match Port and Identify Immediately
- Match Port and Delay Identification
- Match Token and Identify Immediately
- Match Multiple Tokens
- Match Token and Create Metadata

Detailed language information and samples are provided in this topic. This topic describes the XML schema used to define a FlexParse file. The SML node, attribute, and values referenced in descriptive text are **bold**. The root node of every file must be the **parsers** node. Under that node there can be any number of parser nodes. Each parser node defines a single parser.

A parser node can have an optional **declaration** node and any number of **match** nodes.

### Topics

- [Arithmetic Functions](#)
- [Common Parser Operations](#)
- [General Functions](#)
- [Logging Functions](#)

- [Nodes](#)
- [Payload Functions](#)
- [Regex](#)
- [String Functions](#)
- [Lua Parsers](#)

## Arithmetic Functions

This topic defines language for the flex parser arithmetic functions.

This topic defines language for the flex parser arithmetic functions. All numbers are 64-bit unsigned values and subject to both underflow and overflow, depending on the operation.

### Language Definition

The following table provides language definitions.

Node Name	Attribute Name	Description
and		Performs bitwise AND between two numbers.
	name	Variable to AND result into.
	value	Number to AND into result.
or		Performs bitwise OR between two numbers.
	name	Variable to OR result into.
	value	Number to OR into result.
increment		Performs ADDITION of two numbers.
	name	Variable containing the initial value AND to receive ADDITION results.
	value	Number to ADD to initial value.
decrement		Performs SUBTRACTION of two numbers.
	name	Variable containing initial value AND to receive SUBTRACTION results.
	value	Number to SUBTRACT from initial value.
divide		Performs DIVISION of two numbers.

Node Name	Attribute Name	Description
	name	Variable containing the initial value AND to receive DIVISION results.
	value	Number by which to divide the initial value. Division by zero generates an error and stops any further processing of the current session by this parser.
modulo		Performs MODULO of two numbers.
	name	Variable containing the initial value AND to receive MODULO results.
	value	Number by which to divide the initial value. Division by zero generates an error and stops any further processing of the current session by this parser.
multiply		Performs MULTIPLICATION of two numbers.
	name	Variable containing the initial value AND to receive MULTIPLICATION results.
	value	Number by which to MULTIPLY the initial value.
shiftright		Performs a binary shift right.
	name	Variable containing the initial value AND to receive shift results.
	value	Number of bits to shift by.
shiftleft		Performs a binary shift left.
	name	Variable containing the initial value AND to receive shift results.
	value	Number of bits to shift by.

## Common Parser Operations

This topic provides some examples of common parser operations.

This topic includes five common parser operations.

### Match Port and Identify Immediately

```
<?xml version="1.0" encoding="utf-8"?>
<parsers
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="parsers.xsd">
  <parser name="CustApp" desc="Acme Custom App" service="45324">
    <declaration>
      <port name="port" value="45324" />
    <declaration>
      </match name="port">
        <identify />
      </match>
    </parser>
  </parsers>
```

### Match Port and Delay Identification

```
<?xml version="1.0" encoding="utf-8"?>
<parsers
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="parsers.xsd">
  <parser name="MSRPC" desc="Microsoft RPC protocol" service="135">
    <declaration>
      <port name="port" value="135" />
      <number name="state" scope="session" />
      <session name="end" value="end" />
    </declaration>
    <match name="port">
      <assign name="state" value="1" />
    </match>
    <match name="end">
```

```

        <if name="state" equal="1" />
            <identify />
        </if>
    </match>
</parser>
</parsers>

```

### Match Token and Identify Immediately

```

<?xml version="1.0" encoding="utf-8?>
<parsers
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="parsers.xsd">
  <parser name="RDP" desc="Remote Desktop Protocol" service="3389">
    <declaration>
      <token name="signature" value="Cookie: msthash=" />
    </declaration>
    <match name="signature">
      <identify />
    </match>
  </parser>
</parsers>

```

### Match Multiple Tokens

```

<?xml version="1.0" encoding="utf-8"?>
<parsers
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="parsers.xsd">
  <parser name="MyServiceMultiToken" desc="Multiple Tokens"
    service="333">
    <declaration>
      <number name="state" scope="stream" />
      <token name="user" value="USER " />
      <token name="pass" value="PASS " />
      <session name="session" value="end" />
    </declaration>
  </parser>
</parsers>

```



```
<match name="user">
    <or name="state" value="1" />
</match>
<match name="pass">
    <or name="state" value="2" />
</match>
<match name="session">
    <if name="state" equal="3">
        <identify />
    </if>
</match>
</parser>
</parsers>
```

### Match Token and Create Metadata

```
<?xml version="1.0" encoding="utf-8"?>
<parsers xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="parsers.xsd">
    <parser name="SHELL" desc="Command Shell Identification">
        <declaration>
            <token name="cmd.exe" value=" (C) Copyright 1985-2001
Microsoft Corp" options="linestart" />
            <meta name="client" key="client" format="Text" />
        </declaration>
        <match name="cmd.exe"
            <register name="client" value="MS Command Shell" />
        </match>
    </parser>
</parsers>
```

## General Functions

This topic defines language for the flex parser general functions.

### General Functions Language Definition

Node Name	Attribute Name	Description
apptype		Gets the currently defined service type for the current session.
	name	A number variable to receive the current service type.
identify		Marks the session with the parser's service type if the service type has not already been identified.
assign		Assigns a value to a variable.
	name	The unique identifier assigned to the item in the declaration section.
	value	Optional. If specified, the action defined in the match is only applied when the declaration matches the given value.
getmeta		Retrieves the value of meta that generated a callback. This function will return empty results (0, zero length string) if called when there was no meta callback.
	name	The variable to receive the value of the meta that generated the callback.OK.
gettoken		Returns the current matched token.
	name	A string variable to receive the current matched token. If there is no current token, the variable is assigned an empty string.
end		This terminates the execution of the current <b>match</b> section.

Node Name	Attribute Name	Description
if		Compares two values. If the comparison is true, executes any sub-actions. Comparisons can be <b>number</b> or <b>string</b> types, as long as both values are the same type.
	name	The unique variable identifier assigned to the item in the <b>declaration</b> section.
	equal notequal less lessequal greater  greaterequal and or	The operation value to compare. If true, any sub-actions are executed.
register		Adds metadata to the session.
	name	The unique identifier of a meta variable to be created, as defined in the <b>declaration</b> section.
	value	The value of the metadata to be created.
while		Compares two values and executes any sub-actions if the comparison is true. Comparisons can be <b>number</b> or <b>string</b> types, as long as both values are the same type.
	name	The unique variable identifier assigned to the item in the declaration section.

Node Name	Attribute Name	Description
	equal notequal less lessequal greater  greaterequal and or	Specifies the operation value to compare. If true, any sub-action is executed. The <b>and</b> and <b>or</b> attributes signify bitwise operations and can only be applied to <b>number</b> variables.
call		Execute the specified <b>match</b> element. This can be any match element defined in the same flex parser regardless of how it was declared.
	value	<p>The name of the match element, or a string variable containing the name of a match element.</p> <ul style="list-style-type: none"><li>• If the match element name is specified, the parser will not load if the named matched element doesn't exist.</li><li>• If a string variable is specified, the <b>call</b> element will execute any child elements that it may have if the string value resolves to a match element after executing the named match element.</li><li>• If no <b>match</b> element can be found matching the string value, no action is taken.</li></ul>

## Logging Functions

This topic defines language for the flex parser logging functions.

Logging functions provide a means for a flex parser to write to the system log. Logging functions can be extremely useful when creating a new flex parser, but should be kept to an absolute minimum when a flex parser is deployed to a production system.

### Language Definition

Node Name	Attribute Name	Description
failure		Logs a message to the system log with the log level <b>Failure</b> .
	value	A string to include as the log message.
warning		Logs a message to the system log with the log level <b>Warning</b> .
	value	A string to include as the log message.
info		Logs a message to the system log with the log level <b>Info</b> .
	value	A string to include as the log message.
debug		Logs a message to the system log with the log level <b>Debug</b> .
	value	A string to include as the log message.

## Nodes

This topic defines language for the flex parser nodes.

### Nodes Language Definition

Node Name	Attribute Name	Description
<code>parsers</code>		The root node in each definition file.
	<code>xmins:xsi</code>	Defines the namespace to use for the schema inclusion. This attribute is not required; however, language definition is not possible without it. This node must have the following value: <a href="http://www.w3.org/2001/XMLSchema-instance">http://www.w3.org/2001/XMLSchema-instance</a>
	<code>xsi:noNamespaceSchemaLocation</code>	Defines the XSD schema validation file used to validate the language definition. This attribute is not required; however, language definition is not possible without it. This node must have the following value: <code>parsers.xsd</code>
<code>parser</code>		The node that defines a single parser definition. This node must be directly under the <code>parsers</code> node. There can be more than one per file.

Node Name	Attribute Name	Description
	name	The name that uniquely identifies the parser. This name should be short and succinct. This is used by the system to allow enabling and disabling. It should contain only the letters [a-z] and [A-Z].
	desc	This node provides a friendly description of what the parser does.
	service	This is the unique number assigned to the session when identified.
declaration		The node that delineates the definition. Each of these definitions can have an associated <code>match</code> entry.
token		Specifies a definition for identifying a token somewhere in the session protocol. This defines a <code>match</code> callback when the specified tokens are encountered in a session payload. The <code>read</code> position is set to the byte immediately following the matched token.
	name	This is a unique identifier for the declaration.
	value	This is the exact token value to be identified.

Node Name	Attribute Name	Description
	options	Options specify that the token should start on a new line or at an end of a line ( <code>linestart</code> or <code>linestop</code> ).
meta-callback		Registers a callback for the flex parser whenever meta of a specific format is created. This can be further qualified to generate callbacks only for sessions that have been identified as a specific apptype (e.g. 80 for http).
	name	Name of the match element to be executed when a callback occurs. (String)
	key	Name of the meta key that generates callbacks. (String)
	format	The data type of the meta key that will generate the meta.
	apptype	The meta callback is only generated if the session being parsed has been identified with the specified apptype. (Unsigned Integer, Optional)
number		Defines a numeric variable that can be referenced elsewhere within the parser definition. All numeric values are 64-bit unsigned values.



Node Name	Attribute Name	Description
	name	This is a unique identifier for the declaration.
	scope (optional)	Specifies when to reset the variable. This can either be for each side of a two-sided session or only after a new session is detected. The possible values are <b>global</b> , <b>constant</b> , <b>stream</b> , and <code>session</code> (default).
string		Defines a numeric variable that can be referenced elsewhere within the parser definition.
	name	This is a unique identifier for the declaration.
	scope (optional)	Specifies when to reset the variable. This can either be for each side of a two-sided session or only after a new session is detected. The possible values are <b>global</b> , <b>constant</b> , <b>stream</b> , and <code>session</code> (default).
port		Defines a <b>match</b> callback when a session is encountered using the specified port. The <b>read</b> position is set to the first byte of the first stream (client) in the session.
	name	This is a unique identifier for the declaration.

Node Name	Attribute Name	Description
session	value	This is the port number to identify.
		Defines a <code>match</code> callback for session begin/end events. These events only occur if a token for the parser is encountered in the session.
	name	This is a unique identifier for the declaration.
stream	value	Specifies that processing takes place at the beginning of a new session or at the end of a session ( <code>begin</code> or <code>end</code> ).
		Defines a <code>match</code> callback for stream begin/end events. These events only occur if a token for the parser is encountered in the stream.
	name	This is a unique identifier for the declaration
function	value	Specifies that processing takes place at the beginning or at the end of a stream ( <code>begin</code> or <code>end</code> ).
		Defines a <code>match</code> section that can be used as a generic function. No callbacks are associated with this declaration.
	name	This is a unique identifier for the declaration.

Node Name	Attribute Name	Description
meta		Defines the type of data that the parser will create.
	key	Specifies the key name. The key needs to be 1-16 bytes in size.
	format	Specifies the variant type (for example, <b>Text</b> , <b>IPv4</b> , <b>UInt32</b> ). Refer to the SDK documentation for a full list.
pattern		Defines a regular expression variable for use by the <code>regex</code> function
	name	This is a unique identifier for the declaration.
	scope (optional)	Specifies when to reset the variable. This can be for each side of a two-sided session or only after a new session is detected. Possible values are <b>global</b> , <b>constant</b> , <b>stream</b> , and <b>session</b> (default).
	value (optional)	Specifies a regular expression to assign to the pattern variable. This attribute is only valid when the <b>scope attribute</b> is set to <code>constant</code> .

Node Name	Attribute Name	Description
match		<p>The possible entries for taking an action once a match criterion has been found for a declaration. These nodes can be nested to provide deeper logic. There are several categories of execution elements (functions) that can appear as children of a match element:</p> <ul style="list-style-type: none"><li>• General</li><li>• Arithmetic</li><li>• String</li><li>• Payload</li></ul>

## Payload Functions

This topic defines language for the flex parser payload functions.

These functions operate on a `read` position, set at the beginning of a `match` element.

### Language Definition

Node Name	Attribute Name	Description
<code>find</code>		Searches the stream payload starting at the read position for a provided string value. If the value is found, the offset from the read position is returned. Any child elements will then execute. If not found, any child elements will not execute.
	<code>name</code>	A <code>number</code> variable to receive the offset from the <code>read</code> position where the match begins.
	<code>value</code>	A string to find.
	<code>length</code> (optional)	A limit to the length of the payload to be searched. If a limit is not provided, the remainder of the payload is searched. It is recommended to always use the smallest value possible here in order to reduce the effect on performance.
<code>install-decoder</code>		To enable tokens to match on payload data that may be fragmented or otherwise encoded. A scan decoder can be installed to preprocess a section of the payload before it is scanned for tokens. An example would be an HTTP response that uses the chunked transfer encoding with gzip content encoding. By parsing the HTTP header, the necessary type, offset, and length parameters can all be set, after which the HTTP response payload would appear to the token scanning as if neither encoding had been applied. However, this incurs significant overhead.

Node Name	Attribute Name	Description
	type	The type of decoder to install. Valid options are: gzip, deflate, chunked, chunked-gzip, chunked-deflate.
	offset	Offset from the current read position to begin decoding.
	length	The maximum payload length to decode.
isdecoding		Tests whether an installed decoder is currently active. If so, any children of this function will execute. This function has no parameters.
move		Moves the <code>read</code> position forward in the current stream by a specified number of bytes. If there is sufficient data in the stream, the <code>read</code> position is updated and any child elements will then execute. If not found, the <code>read</code> position remains unchanged and any child elements will not execute.
	value	The number of bytes to move the <code>read</code> position.
	direction (optional)	The direction to move the current read position. Can be <code>forward</code> (default) or <b>reverse</b> .
packetid		Returns the id of the packet for the current read position. It is possible for the result to be 0, which indicates that the packet id could not be determined.
	name	A number variable to receive the current packet id.
payload-position		Returns the current read position. This is a zero based index into the stream payload.
	name	A number variable to receive the current read position.

Node Name	Attribute Name	Description
read		Reads a specified number of bytes starting at the <code>read</code> position into a variable. If there is sufficient data in the stream, the <code>read</code> position is updated, the data read assigned, and any child elements will then execute. If not found, the <code>read</code> position remains unchanged and any child elements will not execute.
	name	The name of a <code>string</code> or <code>number</code> variable to receive stream data. If a <code>number</code> variable is provided, the bytes read are interpreted as a single unsigned numeric value.
	length	The number of bytes to read from a stream.
	endianess (optional)	The byte ordering to use when reading into a <code>number</code> variable. Can be <code>big</code> (default) or <code>little</code> . The attribute is invalid when reading into a <code>string</code> variable.

## Regex

This topic defines language for the flex parser regex node.

Regex searches the stream payload starting at the `read` position for matches to a provided regular expression. If matches are found, the offset from the `read` position and, optionally the matched string, is returned. Any child elements execute. If no matches are found, child elements do not execute.

### Language Definition

Attribute Name	Description
<code>name</code>	A <code>number</code> variable to receive the offset from the <code>read</code> position where the match begins.
<code>value</code>	A regular expression to find.
<code>length</code> (optional)	A limit to the length of the payload to be searched. If a limit is not provided, the remainder of the payload is searched. It is recommended to always use the smallest value possible here in order to reduce the effect on performance.
<code>found</code> (optional)	The name of a <code>string</code> variable to receive a matched string.



## String Functions

This topic provides language definitions for the flex parser string functions.

### String Functions Language Definition

Node Name	Attribute Name	Description
append		Attaches a number or string to the end of a <code>string</code> variable.
	name	The unique identifier of a string variable to which the specified value is to be attached.
	value	A number or string to attach.
find		Searches a string for a provided string value. If it is found, the position is returned and any child elements will execute. Otherwise, child elements will not execute.
	name	A <code>number</code> variable to receive the zero-based position, where the provided value string was found in the <b>in</b> string.
	value	A string to find.
	in	A string to search.
	length (optional)	A limit to the length of the <b>in</b> string to be searched. If a limit is not provided, all of <b>in</b> will be searched.
length		Assigns the length of a string to a <code>number</code> variable.
	name	A <code>number</code> variable to receive the length of the specified string.

Node Name	Attribute Name	Description
	value	A string value whose length is to be determined.
regex		Searches a string for matches to the provided regular expression. If a match is found, the position and, optionally, the matching string is returned. Any child elements will then execute. If not found, any child elements will not execute. Regular expression operations can adversely affect system performance.
	name	A number variable to receive the zero-based position, where the provided regular expression matched in the in string.
	value	A regular expression to be searched for.
	in	A string to search.
	length (optional)	A limit to the length of the in string to be searched. If a limit is not provided, all of in will be searched.
	found (optional)	The name of a string variable to receive the matched string.
substring		At least one of the optional attributes from and length must be specified.
	name	The unique identifier of a string variable to receive the extracted value.
	value	A string value from which to extract a substring.
	from (optional)	The zero-based position from which to begin the substring. If not specified, it defaults to zero.

Node Name	Attribute Name	Description
	length (optional)	The number of characters to extract. If not specified, it defaults to the remaining length of the string.
tolower		Converts a string to all lowercase letters.
	name	The name of a <code>string</code> variable to process.
toupper		Converts a string to all uppercase letters.
	name	The name of a <code>string</code> variable to process.
urldecode		Decode a string containing url-encoded characters.
	name	A string variable to receive the decoded string.
	value	A url-encoded string to decode.
base64decode		Decodes a base-64 encoded string.
	name	A string variable to receive the decoded string.
	value	A url-encoded string to decode.
<b>uudecode</b>		Decode a uuencoded string.
	name	A string variable to receive the decoded string.
	value	A uuencoded string. The header and trailing lines should not be included.
quotedprintabledecode		Decode a Quoted-printable encoded string.
	name	A string variable to receive the decoded string.
	value	A quoted-printable encoded string.

Node Name	Attribute Name	Description
convert-ebcdic		Convert an EBCDIC string to its ASCII equivalent.
	name	A string variable to receive the decoded string.
	value	A url-encoded string to decode.

## Geo IP Parser

This topic introduces the Geo IP parser for Decoders.

One of the files available for editing in the Services Config view > Files tab is **GeoPrivate.ipl**, the Geo IP parser.

### GeoPrivate.ipl

The Geo IP parser is a fixed parser that takes IP addresses and converts them to geographical locations. The locations are displayed through the Google Earth display.

The geolocation metadata in **GeoPrivate.ipl**, are added for both **ip.src** and **ip.dst**. The parser uses two external data files, **GeoCity.dat** and **GeoCountry.dat**, which are both stored in the application directory. There are up to eight metadata for each IP address as listed in the table below.

Metadata	Description
city.dst	Destination City
city.src	Source City
country.dst	Destination Country
country.src	Source Country
latdec.dst	Destination Decimal Latitude
latdec.src	Source Decimal Latitude
longdec.dst	Destination Decimal Longitude
longdec.src	Source Decimal Longitude

## Lua Parsers

One of the files available for editing in the Services Config view > Files tab is **NwLua.xml**, the Lua parser.

### List of Lua Parsers

There are a number of Lua parsers available from Live. See [RSA Content](#) for:

- A complete list of these parsers
- Their interdependencies
- The Flex parsers that are subsumed by each Lua parser.

Five common parser operations are:

- Match Port and Identify Immediately
- Match Port and Delay Identification
- Match Token and Identify Immediately
- Match Multiple Tokens
- Match Token and Create Metadata

## Search Parser

This topic explains how to configure a custom parser used on a Decoder to generate metadata by scanning for pre-defined keywords and regular expressions in the Services Config view > Files tab.

One of the files available for editing in the Services Config view > Files tab is **search.ini**, the search parser.

### search.ini

The Search Parser is a custom parser used to generate metadata by scanning for pre-defined keywords and regular expressions. The parser searches the payload of a reconstructed session for string matches and can execute a regular expression search. You can configure the parser by editing the search.ini file.

**Caution:** The search parser can have a significant impact on system performance. It is important that both the search mechanism and the data to which it is applied to be well understood before creating new search definitions and enabling the search parser.

The search definition is used across all protocols. There are three basic search methods:

- Keyword: Search a stream for a specific set of words
- Pattern: Search a stream for a regular expression match
- Keyword + Pattern: Search a stream for a regular expression if it contains any of a given set of keywords.

For a detailed explanation, see Search Parser in the [search.ini Search String Syntax](#).

## search.ini Search String Syntax

This topic introduces search methods and syntax for use in Search parser.

The Search parser uses three basic search methods:

- Keyword: Search a stream for a specific set of words.
- Pattern: Search a stream for a regular expression match.
- Keyword+Pattern: Search a stream for a regular expression if it contains any of a given set of key words.

### Syntax

```
Maxrecon=<max_size>Maxsearch=<max_ssearch_length>MatchLimit=<max_
matches_per_stream
Search Name
Services=<service_id_list>Keywords=<keyword_
list>|Pattern=<expression>Case=0|1
Proximity=<number_of_bytes>Recon=0|1
Raw=0|1
```

### Parameters

Parameters used in this command:

Parameter	Description
autocheck	Automatically fixes all problems without prompting
header Only	Check/display the header of each file
chatty	Displays a hex dump of every object in the file (huge amount of data)
dump#-#	Indicates a zero-based object or range of objects in the file to output in hex to the console

### Example

Following is an example of the command:



To check all NetWitness database files located in the Collection named Default. If any problems are found, the command will describe the problem and ask if you would like to fix it.

```
dbcheck C:\Documents and Settings\User\My Documents\NetWitness\  
Investigations\Default\*.nw*
```

## Wireless LAN Configuration

This topic introduces the wireless LAN configuration file for Decoders, which is in the Services Config view > Files tab.

### **wlan-config.xml**

One of the files available for editing in the Services Config view > Files tab is **wlan-config.xml**, the wireless LAN configuration file.

It controls the 802.11 parsers. Its chief purpose is to control decryption of raw 802.11 frames captured by the Decoder. This file is optional. If decryption of 802.11 traffic is not desired, there is no need to create the file.

There are five link-level parsers related to wireless LAN packet capture:

- IEEE 802.11 parser (data frames and beacons only)
- Radiotap w/ 802.11 header
- Absolute Value Systems (AVS) w/ 802.11 header
- Prism II w/ 802.11 header
- CACE's "Per Packet Information" (PPI) w/ 802.11 header

The 802.11 wireless parsers introduced in 9.8 all share a single configuration file. This wlan - config.xml file is used to define any wireless access points the user may have in the network, and its primary purpose is to control decryption. The BSSID of the access point and the SSID that it's authoritative for is added to this file as well as all of the active default keys used by the access point.



## Decoder and Log Decoder References


---

This is a collection of references, which provide information about the user interface for Decoders and Log Decoders in NetWitness Suite, with references to the procedures that describe the work you can do in that part of the user interface. These topics are presented in alphabetical order.

### Topics

- [Services Config View - Data Retention Scheduler](#)
- [Services Config View - Data Privacy Tab](#)
- [Services Config View - Feeds Tab](#)
- [Services Config View - Files Tab](#)
- [Services Config View - General Tab](#)
- [Services Config View - Parsers Tab](#)
- [Services Config View - Parser Mappings Tab](#)
- [Services Config View - Rules Tabs](#)
- [Services System View - Decoders](#)

## Services Config View - Data Privacy Tab

In the Data Privacy tab (**ADMIN > Services > Select a Decoder or Log Decoder >  > Config > Data Privacy tab**), Administrators can configure data privacy parameters for certain Core services. For the Decoder and Log Decoder, you can set the default hash algorithm and salt.

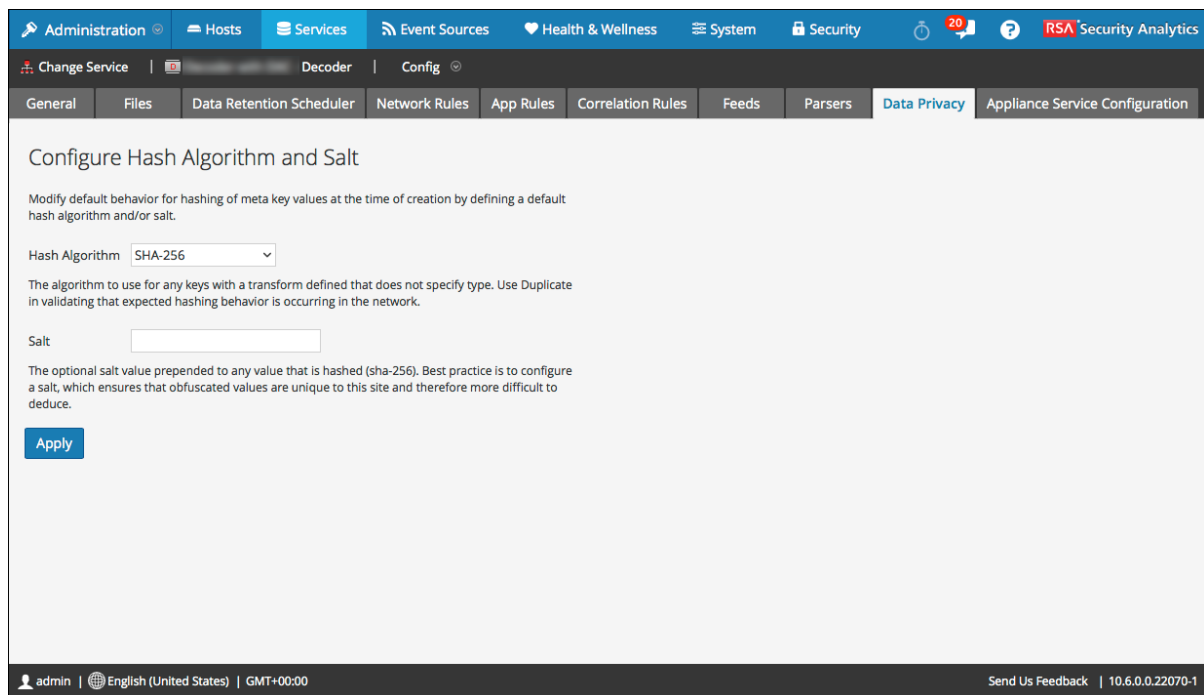
### What do you want to do?

User Role	I want to ...	Documentation
Administrator	configure hash algorithm and salt	"Configure the Hash Algorithm and Salt" in the <i>Data Privacy Management Guide</i> . (Go to the <a href="#">Master Table of Contents</a> for Version 11.0 to find NetWitness Suite 11.0 documents.)

### Related Topics

- [Decoder and Log Decoder Quick Setup](#)
- [Configure Common Settings on a Decoder](#)

## Quick Look





The Data Privacy tab has the Configure Hash Algorithm and Salt configuration settings. The following table describes the parameters in this tab.

Parameter	Description
Hash Algorithm	Displays a drop-down list of hash algorithms to use for any keys with a transform that does not specify algorithm type. Possible values are SHA-256 and Duplicate. Duplicate is a special algorithm available for administrators to use when validating that expected hashing behavior is occurring in the network. In versions of NetWitness Suite prior to 10.5, SHA-1 was available as a hash algorithm, but RSA does not recommend use of SHA-1.
Salt	Indicates the optional salt value prepended to any value that is hashed. Best practices for security purposes dictate a salt value that is no less than 100 bits or 16 characters in length. Configuring a value ensures that obfuscated values are unique to this site and therefore more difficult to deduce. For more information on this field, see "Configure Data Obfuscation" in the <i>Data Privacy Management</i> guide.

Parameter	Description
Apply	Applies any changes.

## Services Config View - Data Retention Scheduler

In the Services Config View Data Retention Scheduler tab, you can set the rollover criteria for removing database records from primary storage using an age-based threshold. You can also schedule the timing to check whether the threshold is reached.

To access the Data Retention Scheduler tab, go to ADMIN > Services > select a Decoder or Log Decoder service and click   > View > Config > Data Retention tab.

### What do you want to do?

User Role	I want to...	Documentation
Administrator	Schedule the timing to see if the threshold is reached.	<a href="#">Configure Transaction Handling on a Decoder</a>

### Related Topics

- [Configure Common Settings on a Decoder](#)
- [Decoder and Log Decoder Quick Setup](#)

### Quick Look

This is an example of the Data Retention Scheduler tab.

Define the rollover criteria for removing database records from primary storage using an age-based threshold, and schedule the timing for checking if the threshold has been reached.

Threshold **1** → ☒ Duration ☐ Date **2**

Days  Hours  Minutes

Run **3** → ☒ Interval ☐ Date & Time **4**

Hours  Minutes

**Apply** **Reset**

RSA | NETWITNESS SUITE 11.0.0.0-170907142902.1.2d50a0a

- 1 Threshold Duration:** Removes database files older than the selected number of days, minutes, or hours.
- 2 Threshold Date:** Removes database files older than the selected UTC date (YYYY-MM-DD-HH:MM:SS) that are not compatible with minutes, hours, or days parameters.
- 3 Run Interval:** Indicates the number of hours between executions.
- 4 Run Date and Time:** Defines which days of the week to execute the scheduler, as well as time of execution in HH:MM:SS format for the local time of the service.




## Services Config View - Feeds Tab

Feeds and parsers are Lua programs loaded and compiled when either processing capture files in Investigation or capturing data with Decoders. Most commonly, they are used for static meta extraction and service identification.

**Note:** Pre-11.0 versions of NetWitness used FLEXPARE programs in addition to Lua programs; Flexparsers are deprecated in NetWitness Suite 11.0. Unless otherwise stated, any reference to Decoders applies to Log Decoders as well.

NetWitness Suite uses feeds to create metadata based on externally defined meta values. A feed is a list of data that is compared to sessions as they are captured or processed. For each hit, additional metadata is created. This data can identify and classify malicious IPs or incorporate additional information such as department and location based on internal network assignments. Some examples of feeds include threat feeds to identify BOTNets, DHCP mappings, or even active directory information such as physical location or logical department.

Feeds can be added, removed, and updated while a Decoder is running without affecting capture. The Feeds tab (**ADMIN > Services > select a service and click  > View > Config > Feeds tab**) provides a user interface for managing feeds on Decoders.

### What do you want to do?

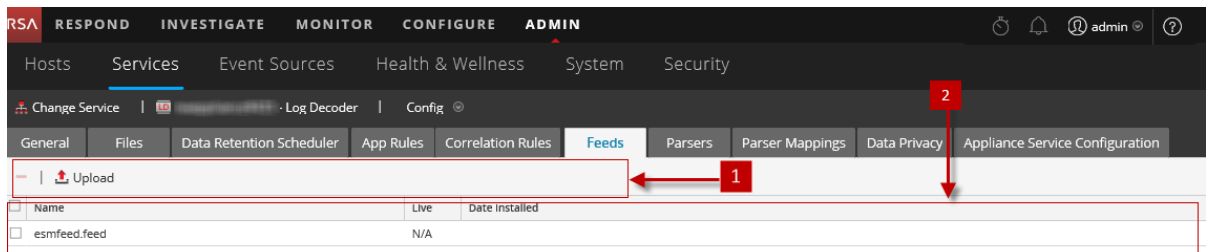
User Role	I want to...	Documentation
Administrator	configure feeds	<a href="#">Configure Feeds and Parsers</a>
Administrator	enable and disable parsers	<a href="#">Enable and Disable Parsers and Log Parsers</a>

### Related Topics

- [Configure Common Settings on a Decoder](#)
- [Decoder and Log Decoder Quick Setup](#)
- [Upload Feeds Dialog](#)
- [Feed and Parser References](#)

### Quick Look



This is an example of the Feeds tab.



1 Feeds Tab Toolbar - Provides options to work with feeds in the grid

2 Feed Grid - Lists all feeds that are currently deployed on the Decoder

### Feeds Tab Toolbar

Feature	Description
 Upload	Displays the Upload Feeds dialog.
	Deletes the selected feeds.

### Feeds List

The Feeds list provides a listing of all currently deployed feeds for the Decoder.

Column	Description
<b>Name</b>	The name of the feed or the feed file.
<b>Live</b>	Indicates if the feed originated from Live. Possible values are <b>Yes</b> , <b>No</b> , or <b>N/A</b> . <ul style="list-style-type: none"> <li><b>Yes</b> = Installed through Live</li> <li><b>No</b> = Installed through NetWitness Suite</li> <li><b>N/A</b> = The feed has no attributes file created by NetWitness Suite to track the installation date. The feed may have been installed manually, not through NetWitness Suite or Live Services. Manually installed feeds still function properly.</li> </ul>
<b>Date Installed</b>	The date the feed was pushed to the service.

## Upload Feeds Dialog

This topic describes the features of the Upload Feeds dialog in the Services Config view > Feeds tab.

The **Upload** option in the Services Config view > Feeds tab displays the Upload Feeds Dialog, in which you can manage the uploading of feeds to a Decoder or Log Decoder.

### What do you want to do?

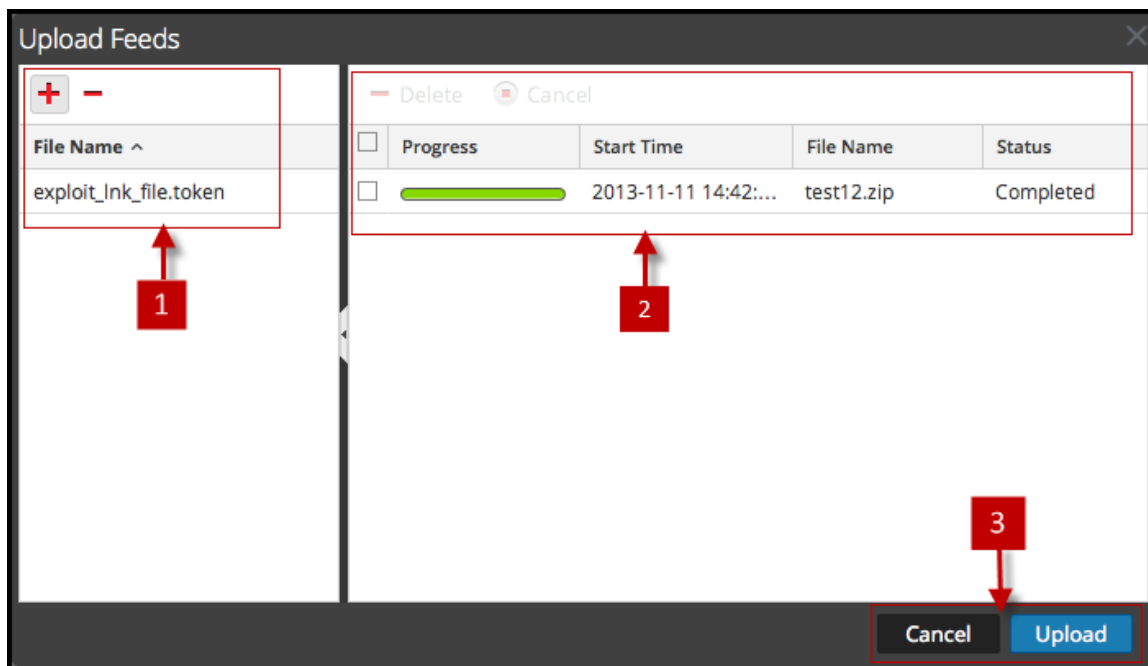
User Role	I want to...	Documentation
Administrator	prepare a list of feeds for upload	<a href="#">Edit, Upload, or Remove a Feed</a>
Administrator	view and delete upload jobs	<a href="#">Edit, Upload, or Remove a Feed</a>

### Related Topics

- [Decoder and Log Decoder Quick Setup](#)
- [Configure Common Settings on a Decoder](#)
- [Feed and Parser References](#)

### Quick Look

This is an example of the Upload Feeds dialog.



- 1 File List - Provides place to prepare a list of feeds for uploading
- 2 Upload Job List - Provides a view of upload jobs
- 3 Upload Feeds Dialog Buttons


### File List

The File List is the place to prepare a list of feeds for uploading. You can add files from a directory structure, and delete files from the grid if you decide that you don't want to upload a particular file. When the list is ready, clicking **Upload** starts the upload process.

Feature	Description
+	Opens a view of the directory structure where you can select files to add to the File list.
-	Deletes the selected files from the File list.
<b>File Name</b>	Lists the feed files you have added from a file system in preparation for uploading to a Decoder. When you click <b>Upload</b> , the files listed here are uploaded.

### Upload Job List

The Upload Job list provides a view of upload jobs started by clicking **Upload**.

Feature/Column	Description
 <b>Delete</b>	Deletes an upload job.
<b>Progress</b>	Displays progress of an upload job.
<b>Start Time</b>	Displays the start time of an upload job.
<b>File Name</b>	Lists filename of the feed being uploaded.
<b>Status</b>	Displays the status of upload job.

**Upload Feeds Dialog Buttons**

Feature	Description
<b>Cancel</b>	Closes the Upload Feed dialog.
<b>Upload</b>	Starts uploading the feed files listed in the File list. Each feed is listed in a separate row in the Upload Process list.

## Services Config View - Files Tab

The Decoder and Log Decoder configuration files are visible and editable in the Services Config view > Files tab. "Edit Core Services Configuration Files" in the *Hosts and Services Getting Started Guide* provides general instructions for editing files. (Go to the [Master Table of Contents](#) for Version 11.0 to find NetWitness Suite 11.0 documents.)

Like other Core services, both the Decoder and Log Decoder have an index file, and may also have a crashreporter, netwitness, and scheduler. The Decoder and Log Decoder index files are named `index-decoder-custom.xml` and `index-logdecoder-custom.xml`.

**Note:** This file type is available only for Log Decoder with Envision content installed. `table-map.xml` and `table-map-custom.xml` will now show up but only if `table-map.xml` was found on the file system (for example, it is a log decoder with envision content installed).

### What do you want to do?

User Role	I want to...	Documentation
Administrator	obtain log files from pre-11.0 Log Decoder	<a href="#">Obtain Log Files a from Pre-11.0 Log Decoder</a>
Administrator	edit files and parsers	<a href="#">Feed and Parser References</a>

### Related Topics



- [Configure Common Settings on a Decoder](#)
- [Decoder and Log Decoder Quick Setup](#)
- [Create Custom Meta Keys Using a Custom Feed](#)

### Quick Look

Filename	Description
<code>GeoPrivate.ipl</code>	This fixed parser takes the IP addresses and converts them to geographical locations. The locations are displayed through the Google Earth display.

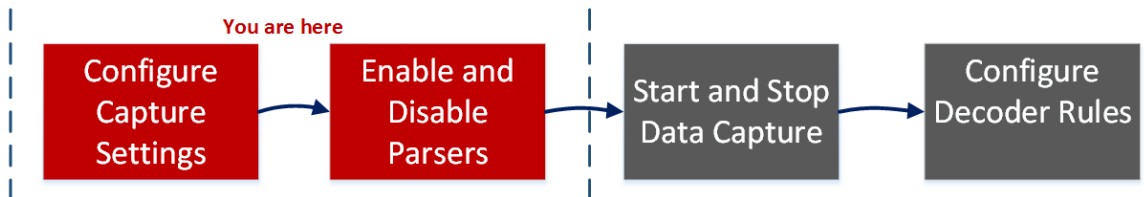
Filename	Description
feed-definitions.xml	Used to create custom feeds, this is the XML schema used by the Decoder to define a <b>feed</b> message when it creates a <b>.feed</b> file.
traffic_flow_options.lua	Used to provide directionality information. Update this file with environment-specific internal and external subnets for the Lua parser to create proper directionality in metadata. The parser is described in <a href="#">RSA Content for RSA NetWitness Suite</a> .
search.ini	This is the Search Parser configuration file. The Search Parser is a custom parser, used to generate metadata by scanning for pre-defined keywords and regular expressions.
wlan-config.xml	This is the wireless LAN configuration file (9/9/2009). This file controls the 802.11 parsers. Its chief purpose is to control decryption of raw 802.11 frames captured by the Decoder.

## Services Config View - General Tab

The General tab for a Decoder in the Services Config view provides a way to manage basic service configuration, configure data capture, and select the parsers that are applied to the captured data. To access the General tab, go to **ADMIN > Services** > select a Decoder or Log Decoder and click   > **View > Config > General tab**.

### Workflow

The following figure depicts common Decoder configuration tasks with the steps you can complete in this view highlighted.



### What do you want to do?

User Role	I want to...	Documentation
Administrator	<b>configure capture settings*</b>	<a href="#">Configure Capture Settings</a>
Administrator	<b>manage parsers and log parsers*</b>	<a href="#">Enable and Disable Parsers and Log Parsers</a>
Administrator	start and stop data capture	<a href="#">Start and Stop Data Capture</a>
Administrator	configure rules	<a href="#">Configure Decoder Rules</a>

\*You can complete these tasks here.

### Related Topics

- [Decoder and Log Decoder Quick Setup](#)
- [Configure Common Settings on a Decoder](#)
- [Configure Feeds and Parsers](#)

### Quick Look

The first figure is an example of the General tab for a Decoder. The second is the General tab for a Log Decoder.



RESPOND INVESTIGATE MONITOR CONFIGURE ADMIN

HOSTS SERVICES EVENT SOURCES HEALTH & WELLNESS SYSTEM SECURITY

Change Service | Decoder | Config

General Files Data Retention Scheduler Network Rules App Rules Correlation Rules Feeds Parsers Data Privacy Appliance Service Configuration

### System Configuration

Name	Config Value
Compression	0
Port	50004
SSL FIPS Mode	<input type="checkbox"/>
SSL Port	56004
Stat Update Interval	1000
Threads	20

### Decoder Configuration

Name	Config Value
<b>Adapter</b>	
Berkeley Packet Filter	
Capture Interface Selected	packet_mmap_io
<b>Cache</b>	
Cache Directory	/var/netwitness/decoder/cache
Cache Size	4 GB
<b>Capture Settings</b>	
Assembler Maximum Size	32 MB
Assembler Minimum Size	0
Assembler Session Flush	1
Assembler Session Pool	50000
Assembler Timeout Packets	60
Assembler Timeout Session	60
Capture Autostart	<input type="checkbox"/>
Capture Buffer Size	32 MB
Parse Maximum Bytes	128 KB
Parse Minimum Bytes	1 KB
Parse Threads	0
<b>Database Max File Sizes</b>	

### Parsers Configuration

Specify if relevant meta data is generated to disk (Enabled), generated only in memory for other Decoder content use (Transient), or not generated at all (Disabled).

Name	Config Value
AIM	Enabled
AIM_lua	Enabled
ALERTS	Enabled
apt_artifacts	Enabled
Avamar	Enabled
BGP_lua	Enabled
BITS	Enabled
bittorrent_lua	Enabled
Canon_BjNP	Enabled
china_chopper	Enabled
creditcard_detection_lua	Enabled
db2_lua	Enabled
DCERPC	Enabled
Derusbi_Server_Handshake	Enabled
DHCP	Enabled
DHCP_lua	Enabled
DNP3_lua	Enabled
DNS	Enabled
DNS_verbose_lua	Enabled
dr_watson_lua	Enabled
duqu_lua	Enabled
DynDNS	Enabled
ein_detection_lua	Enabled
Entropy	Enabled
ethernet_oui	Enabled
Evilgrab	Enabled
exif	Enabled

Apply

1 2 3

Change Service | Log Decoder | Config

General Files Data Retention Scheduler App Rules Correlation Rules Feeds Parsers Data Privacy Appliance Service Configuration

### System Configuration

Name	Config Value
Compression	0
Port	50002
SSL FIPS Mode	<input type="checkbox"/>
SSL Port	56002
Stat Update Interval	1000
Threads	20

### Log Decoder Configuration

Name	Config Value
<b>Adapter</b>	
Berkeley Packet Filter	
Capture Interface Selected	
<b>Cache</b>	
Cache Directory	/var/netwitness/cache
Cache Size	4 GB

### Parsers Configuration

Specify if relevant meta data is generated to disk (Enabled), generated only in memory for other Decoder content use (Transient), or not generated at all (Disabled).

Name	Config Value
ALERTS	Enabled
BITTORRENT	Enabled
FeedParser	Enabled
FIX	Enabled

### Service Parsers Configuration

Enable All Disable All

Name	Config Value
accurev	<input checked="" type="checkbox"/>
actiancevantage	<input checked="" type="checkbox"/>
actidentity	<input checked="" type="checkbox"/>
aforecloudlink	<input checked="" type="checkbox"/>
airdefense	<input checked="" type="checkbox"/>
airmagnet	<input type="checkbox"/>
aix	<input checked="" type="checkbox"/>

Apply

1 2 3 4

- 1 System Configuration - Manages service configuration for a Decoder.
- 2 Decoder Configuration or Log Decoder Configuration - Lets you view and edit service configuration parameters for a Decoder or Log Decoder.
- 3 Parsers Configuration - Lets you select parsers to use on the Decoder.
- 4 Service Parsers Configuration (Log Decoders only) - Lets you select service parsers to use on the Log Decoder.

### System Configuration Section

The System Configuration section manages service configuration for a Decoder. When a service is first added, default values are in effect and should be changed only in special circumstances, for example, if Customer Support advises a change.

System Configuration	
Name	Config Value
Compression	0
Port	50004
SSL FIPS Mode	<input type="checkbox"/>
SSL Port	56004
Stat Update Interval	1000
Threads	20

The System Configuration section has these parameters.

Parameter	Description
<b>Compression</b>	The minimum number of bytes that must be transmitted per response before compression. A setting of 0 disables compression. The default value is <b>0</b> . A change in value is effective immediately for all subsequent connections.
<b>Port</b>	Determines the port used by the service. <div><b>Note:</b> If you change the port number, ensure that you restart the service.</div>
<b>SSL FIPS mode</b>	If enabled, all the data transferred in the network will be encrypted using SSL.
<b>SSL Port</b>	Indicates the port used for encrypting using SSL.



Parameter	Description
<b>Stat Update Interval</b>	<p>The number of milliseconds between statistic updates on the system. Lower numbers cause more frequent updates and can slow down other processes.</p> <p>The default value is <b>1000</b>.</p> <p>A change in value is effective immediately.</p>
<b>Threads</b>	<p>The number of threads in the thread pool to handle incoming requests. A setting of <b>0</b> lets the system decide.</p> <p>A change takes effect on service restart.</p>

### Decoder Configuration Section

The Decoder Configuration section provides a way to view and edit service configuration parameters for a Decoder or Log Decoder. When a service is first added, default values are in effect. You can edit these values to manage traffic capture.

Decoder Configuration	
Name	Config Value
<b>Adapter</b>	
Berkeley Packet Filter	
Capture Interface Selected	
<b>Cache</b>	
Cache Directory	/var/netwitness/decoder/cache
Cache Size	4 GB
<b>Capture Settings</b>	
Assembler Maximum Size	32 MB
Assembler Minimum Size	0
Assembler Session Flush	1
Assembler Session Pool	50000
Assembler Timeout Packets	60

Scrolling to the bottom of the section reveals these additional Decoder Configuration parameters.

Decoder Configuration	
Name	Config Value
Assembler Timeout Session	60
Capture Autostart	<input type="checkbox"/>
Capture Buffer Size	32 MB
Parse Maximum Bytes	128 KB
Parse Minimum Bytes	1 KB
Parse Threads	0
 <b>Database Max File Sizes</b>	
Meta File Size	3 GB
Packet File Size	4 GB
Session File Size	512 MB
 <b>Hash</b>	
Hash Directory	

### Adapter Section

Adapter parameters configure the network interface for capture as described in [Configure Capture Settings](#).

### Cache Section

Cache parameters configure the cache directory and size for session cache files. The following table describes the cache settings. When a service is first added, default values are in effect and should be changed only in special circumstances, for example, if Customer Support advises a change.

Cache Parameter	Description
<b>Cache Directory</b>	The directory where session cache files are stored. The default value is <code>/var/netwitness/decoder/cache</code> . Change takes effect immediately.
<b>Cache Size</b>	The maximum size, in Megabytes (MB), that all files in the cache directory can attain before the oldest files are deleted. Once the threshold is reached, the cache size is reduced by 10%. The default value is <b>4 GB</b> . Change takes effect immediately.

## Capture Settings Section

The Capture Settings section provides a way to configure operational capture settings. When a service is first added, default values are in effect and should be changed only in special circumstances, for example, if Customer Support advises a change.

Capture Settings Parameter	Description
<b>Assembler Maximum Size</b>	Specifies the maximum size in bytes that a session's packet data size can attain. The default value is <b>32 MB</b> . Change takes effect immediately.
<b>Assembler Minimum Size</b>	Specifies the minimum size in bytes that a session must have in order to generate metadata. A value of <b>0</b> means every session has metadata generated. The default value is <b>0</b> . Change takes effect immediately.
<b>Assembler Session Flush</b>	<p>Specifies whether a session is removed from the assembler when the session's last chain is removed from the assembler. The default value is <b>1</b>.</p> <ul style="list-style-type: none"> <li>• <b>2</b> = if the first packet of a session times out of assembler, the session is removed from assembler after parsing is complete. Any subsequent packets for this session create a new session in assembler.</li> <li>• <b>1</b> = If the last chain of a session times out of assembler, the session is removed from assembler. Any subsequent packets for this session create a new session in assembler.</li> <li>• <b>0</b> = If the last chain of a session times out of assembler, the session is left in assembler until it times out. Any subsequent packets for this session are filtered</li> </ul> <p>Change takes effect on service restart.</p>
<b>Assembles Session Pool</b>	Specifies the number of entries in the session pool. The default value is <b>350000</b> . Change takes effect on service restart.

Capture Settings Parameter	Description
<b>Assembler Timeout Packets</b>	Specifies the number of seconds before a packet or chain is timed out. The default value is <b>60</b> . Change takes effect immediately.
<b>Assembler Timeout Session</b>	Specifies the number of seconds before a session is timed out. Default value is <b>60</b> . Change takes effect immediately.
<b>Capture Autostart</b>	Specifies whether capture begins automatically each time Decoder is started. When checked, the value = yes. When unchecked, the value = no. The default value is <b>no</b> . Change takes effect immediately.
<b>Capture Buffer Size</b>	The capture memory buffer allocation in Megabytes. Default value is <b>64 MB</b> . Change takes effect on service restart.
<b>Parse Maximum Bytes</b>	The maximum number of bytes to scan a stream for additional tokens. When the first token is found, the stream is scanned up to the set number of bytes, but no further. A setting of <b>0</b> removes the early termination and the full stream is scanned regardless of size. The default value is <b>128 KB</b> . Change takes effect immediately.
<b>Parse Minimum Bytes</b>	The minimum number of bytes to scan a stream for the first token. If no token is found within the set number of bytes, scanning is terminated. A setting of <b>0</b> removes the early termination and the full stream is scanned regardless of size. The default value is <b>1 KB</b> . Change takes effect immediately.
<b>Parse Threads</b>	The number of parse threads to use for session parsing. A value of <b>0</b> means let the server decide. The default value is <b>0</b> . Change takes effect on service restart.

### Database Max File Sizes Section

The Database Max File Sizes section controls the maximum file size for various databases. When a service is first added, default values are in effect and should be changed only in special circumstances, for example, if Customer Support advises a change.

File Size Parameter	Description
<b>Meta File Size</b>	The maximum size of meta database files in Megabytes. The default value is <b>10 MB</b> . Change takes effect on service restart.
<b>Packet File Size</b>	The maximum size of packet database files in Megabytes. The default value is <b>10 MB</b> . Change takes effect on service restart.
<b>Session File Size</b>	The maximum size of session database files in Megabytes. The default value is <b>100 MB</b> . Change takes effect on service restart.













### Hash Section

The Hash section settings control data base file hashing options. There is a small performance penalty when hashing.

Hash Parameter	Description
<b>Hash Directory</b>	The server directory where all hash files are written. If empty, each hash file is written to the same directory as the file being hashed. The default value is blank. Change takes effect on service restart.

### Parsers Configuration Panel

The Parsers Configuration panel provides a way to select parsers to use on the Decoder. Within some parsers, you can also configure the metadata that the parser creates. See [Enable and Disable Parsers and Log Parsers](#) for detailed information and procedures.

Parsers Configuration		Enable All	Disable All
Specify if relevant meta data is generated to disk (Enabled), generated only in memory for other Decoder content use (Transient), or not generated at all (Disabled).			
Name	Config Value		
 <b>AIM</b>	Enabled		
 <b>ALERTS</b>	Enabled		
BITTORRENT	Enabled		
 <b>DHCP</b>	Enabled		
 <b>DNS</b>	Enabled		
FeedParser	Enabled		
FIX	Enabled		
 <b>FTP</b>	Enabled		
 <b>GeolIP</b>	Enabled		
GNUTELLA	Enabled		
 <b>GTalk</b>	Enabled		
 <b>H323</b>	Enabled		
 <b>HTTP</b>	Enabled		
 <b>HTTPS</b>	Enabled		
 <b>IMAP</b>	Enabled		
 <b>IRC</b>	Enabled		

### Service Parsers Configuration Section for Log Decoder

The Service Parsers Configuration section provides a way to select Service parsers to use on the Log Decoder.



Service Parsers Configuration		Enable All	Disable All
Name	Config Value		
accurev	<input checked="" type="checkbox"/>		
actiancevantage	<input checked="" type="checkbox"/>		
actividentity	<input checked="" type="checkbox"/>		
aforecloudlink	<input checked="" type="checkbox"/>		
airdefense	<input checked="" type="checkbox"/>		
airmagnet	<input type="checkbox"/>		
airtightmc	<input checked="" type="checkbox"/>		
aix	<input checked="" type="checkbox"/>		
alcatelomniswitch	<input checked="" type="checkbox"/>		
apache	<input checked="" type="checkbox"/>		
apachetomcat	<input type="checkbox"/>		

## Services Config View - Parsers Tab

In the Services Config View > Parsers tab, you can view deployed parsers on a Decoder or Log Decoder, upload parsers, and delete deployed parsers. Parsers can be added and removed while a Decoder or Log Decoder is running without affecting capture.

To access the Parsers tab, go to ADMIN > Services > select a Decoder or Log Decoder service and click  > View > Config > Parsers tab.

### What do you want to do?

User Role	I want to...	Documentation
Administrator	View deployed parsers.	<a href="#">Enable and Disable Parsers and Log Parsers</a>
Administrator	Upload parsers to a Decoder or Log Decoder.	<a href="#">Enable and Disable Parsers and Log Parsers</a>

## Related Topics

- [Decoder and Log Decoder Quick Setup](#)
- [Configure Common Settings on a Decoder](#)
- [Upload and Delete Custom Parsers](#)

## Quick Look

This is an example of the Parsers tab. The Parsers grid lists all parsers that are currently deployed on the Decoder.

Name	Live	Date Installed
traffic_flow_options.lua	N/A	
traffic_flow.luax	N/A	

**1 Name:** The name of the parser or the parser file.



**2 Live:** Indicates if the parser originated from Live. Possible values are **Yes**, **No**, or **N/A**.

- **Yes** = Installed through Live Services.
- **No** = Installed through NetWitness.
- **N/A** = The parser has no attributes file created by NetWitness to track the installation date. The parser may have been installed manually, not through NetWitness or Live Services.

**3 Date Installed:** The date the parser was pushed to the service.



**Parsers Tab Toolbar**

The Parsers Tab toolbar has options to work with parsers in the grid.

Feature	Description
 Upload	Enables you to upload parsers to a Decoder or Log Decoder.
	Requests confirmation that you want to delete the selected parsers. You can select <b>No</b> to cancel the deletion, or select <b>Yes</b> to delete the selected parsers.

## Services Config View - Parser Mappings Tab

This topic provides a description of the configurable options for a Log Decoder in the Parser Mappings tab.

In the Parser Mappings Administrators can configure log parser mappings for Log Decoder services. To access the Parser Mappings tab, go to ADMIN > Services > select a service and click   > View > Config > Parser Mappings tab.

**Note:** You can also configure log parser mappings for Log Decoder services by navigating to **ADMIN > Services > Event Sources > Discovery**.

This feature is intended to track a subset of Event Sources that is parsing against the wrong parser.

### What do you want to do?

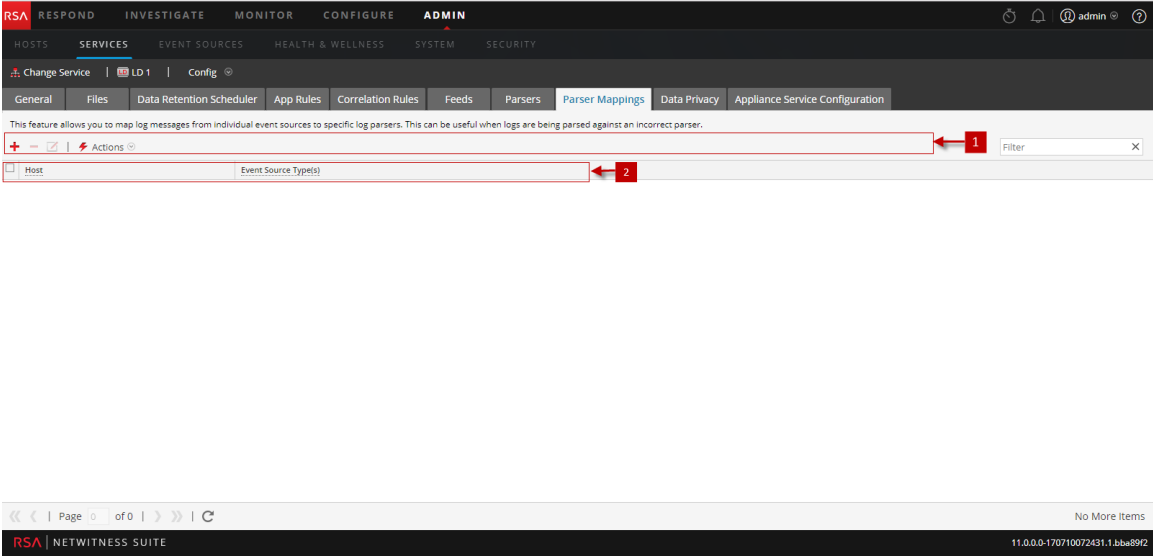
User Role	I want to...	Documentation
Administrator	Manage IPs for Event Source Mapping.	<a href="#">Enable Parser Mappings</a>

### Related Topics

- [Decoder and Log Decoder Quick Setup](#)
- [Configure Common Settings on a Decoder](#)

### Quick Look






This is an example of the tab.



- 1 Parser Mappings Toolbar - Provides options to work with parser mappings in the grid
- 2 Parser Mappings Grid - Lists all parsers that are currently mapped on the Log Decoder

### Parser Mappings Toolbar

The Parser Mappings toolbar has options to work with parser mappings in the grid.

Feature	Description
	Add a parser mapping.
	Delete the selected parser mapping.
	Edit a parser mapping.
	Refresh the list of parser mappings.
	Display the Actions menu. <ul style="list-style-type: none"><li>• <b>Import</b> - Import a parser mapping to a file.</li><li>• <b>Export</b> - Save a parser mapping to a file.</li></ul>

### Parser Mappings List



The Parser Mappings list displays all parsers that are currently mapped on the Log Decoder.

Parameter	Description
Host	Displays the IP address of the host.
Event Source	Displays the Event Sources that are parsing incorrectly.

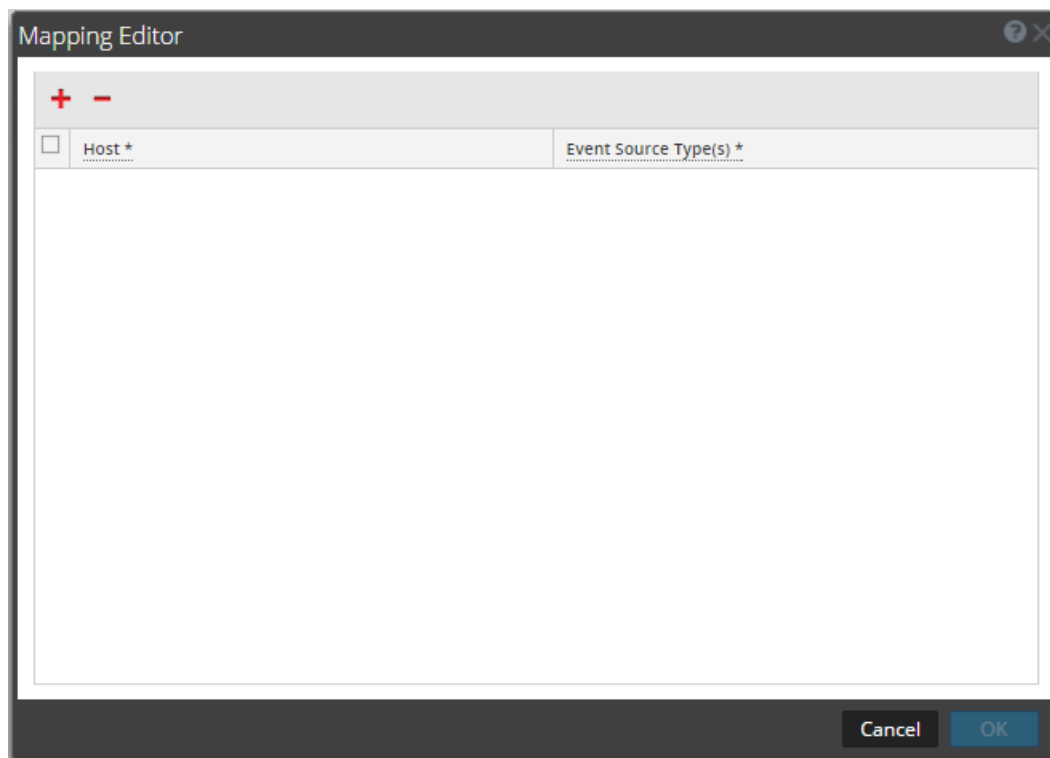
### Parser Mappings Editor Dialog

The Parser Mappings Editor dialog allows you to update an IP to event source mapping.

To access the Parser Mappings Editor dialog, follow these steps:


1. In the NetWitness Suite menu, select **ADMIN > Services**.
2. Select a **Log Decoder**, and in the **Actions** column, select  > **View > Config**.  
The Services Config view is displayed.
3. Select the **Parser Mappings** tab.
4. Click .

The Mapping Editor dialog is displayed.



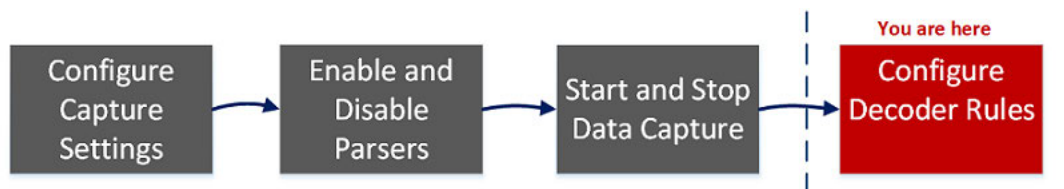
For more information on the Parser Mapping Editor dialog, refer to [Enable Parser Mappings](#).

## Services Config View - Rules Tabs

The Rules tabs in the Services Config view (**ADMIN > Services > select a service and click  > View > Config**) enable you to define and manage capture rules. Each type of rule has a grid with slightly different columns and different parameters in the Rule Editor dialog. Application and correlation rules apply to both Decoders and Log Decoders. Network rules apply only to packet Decoders.

### Workflow

The following figure depicts the workflow for common Decoder configuration tasks with the steps you can complete in this view highlighted.



### What do you want to do?

User Role	I want to...	Documentation
Administrator	configure capture settings	<a href="#">Configure Capture Settings</a>
Administrator	manage parsers and log parsers	<a href="#">Enable and Disable Parsers and Log Parsers</a>
Administrator	start and stop data capture	<a href="#">Start and Stop Data Capture</a>
Administrator	<b>configure rules*</b>	<a href="#">Configure Decoder Rules</a>
Administrator	<b>import, export, or push a rule*</b>	<a href="#">Configure Decoder Rules</a>
Administrator	<b>enable or disable a rule*</b>	<a href="#">Configure Decoder Rules</a>
Administrator	<b>add, edit, or delete a rule*</b>	<a href="#">Configure Decoder Rules</a>

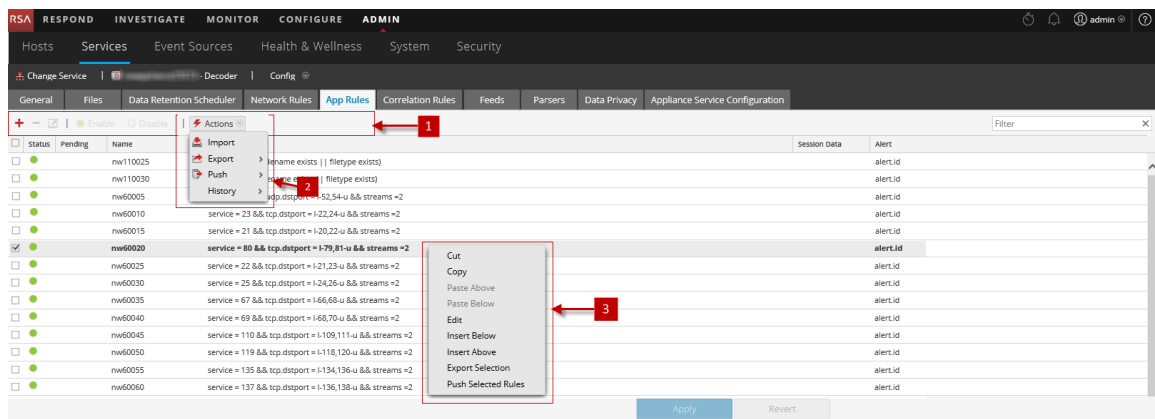
\*You can complete these tasks here.

## Related Topics

- [Configure Common Settings on a Decoder](#)
- [Decoder and Log Decoder Quick Setup](#)
- [App Rules Tab](#)
- [Correlation Rules Tab](#)
- [Network Rules Tab](#)

## Quick Look

This is an example of the App Rules tab.



1 Rules Tab Toolbar - Provides options to work with rules in the grid

2 Rules Actions Menu - Provide options to manage sets of rules

3 Rules List Context Actions - Displays the Rules List Context Menu


## Rules Tab Toolbar

The toolbar is the same for all Config view > Rules tabs.



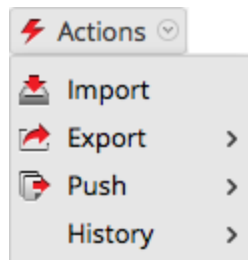
Feature	Description
Actions	Displays the <b>Actions</b> menu.
+	Adds a new rule to a service.
-	Deletes a rule from a service.



Feature	Description
	Allows rule modification.
<input type="radio"/> Disable	Disables a rule (without deleting the rule).
<input checked="" type="radio"/> Enable	Enables (reactivates) a rule.
Filter	The input field for a search string. NetWitness Suite filters the rules dynamically as you type a search string. Clicking <b>x</b> clears the input field, restoring the unfiltered view.
Apply	Saves the changes made to rules and applies the configured rules to a service. Until you apply changes, it is possible to reload the rules as they were before current modifications.
Revert	Discards unsaved changes to the grid and reverts to the unedited rules.

### Rules Actions Menu

The Actions menu has options that help to manage sets of rules.



Option	Description
Import	Imports a set of rules into the user interface so that it can be applied to a service. You can edit the rules before applying.
Export	Saves selected rules or all rules to an .nwr file on the client machine.


Option	Description
Push	<p>Allows rules to be applied to other services (Decoders or Log Decoders) or Decoders belonging to a service group. When pushing, the rules can either be merged (update existing rules and append new ones) or replaced.</p> <ul style="list-style-type: none"> <li>• <b>Push &gt; All.</b> Pushes all rules to other services. All rules on the target services are removed and replaced with all of the rules on the source service.</li> <li>• <b>Push &gt; Selection.</b> Pushes selected rules to other services. You have two options: <ul style="list-style-type: none"> <li>• <b>Replace.</b> Deletes all rules on the target services and replaces them with the selected rules from the source service.</li> <li>• <b>Merge.</b> Merges the selected rules with the existing rules on the target services</li> </ul> </li> </ul>
History	Displays the last ten snapshots of rules applied through NetWitness Suite. You can select and apply (restore) a snapshot to the Decoder at anytime.

### Rules List Context Actions

Within a rules grid, right-clicking a row displays the Rules Grid Context Menu.

Option	Description
Cut	Deletes the current rule.
Copy	Copies the current rule.
Paste Above	Pastes the copied rule above the current rule.
Paste Below	Pastes the copied rule below the current rule.
Edit	Edits the current rule.
Insert Below	Inserts imported rules below the current rule.
Insert Above	Inserts imported rules above the current rule.
Export Selection	Exports the selected rules.
Push Selected Rules	Pushes the selected rules to other services.

## App Rules Tab

The App Rules tab (**ADMIN > Services > select a Decoder or Log Decoder and click  > View > Config > App Rules tab**) enables you to manage application rules. NetWitness Suite applies application rules at the session level.

### What do you want to do?

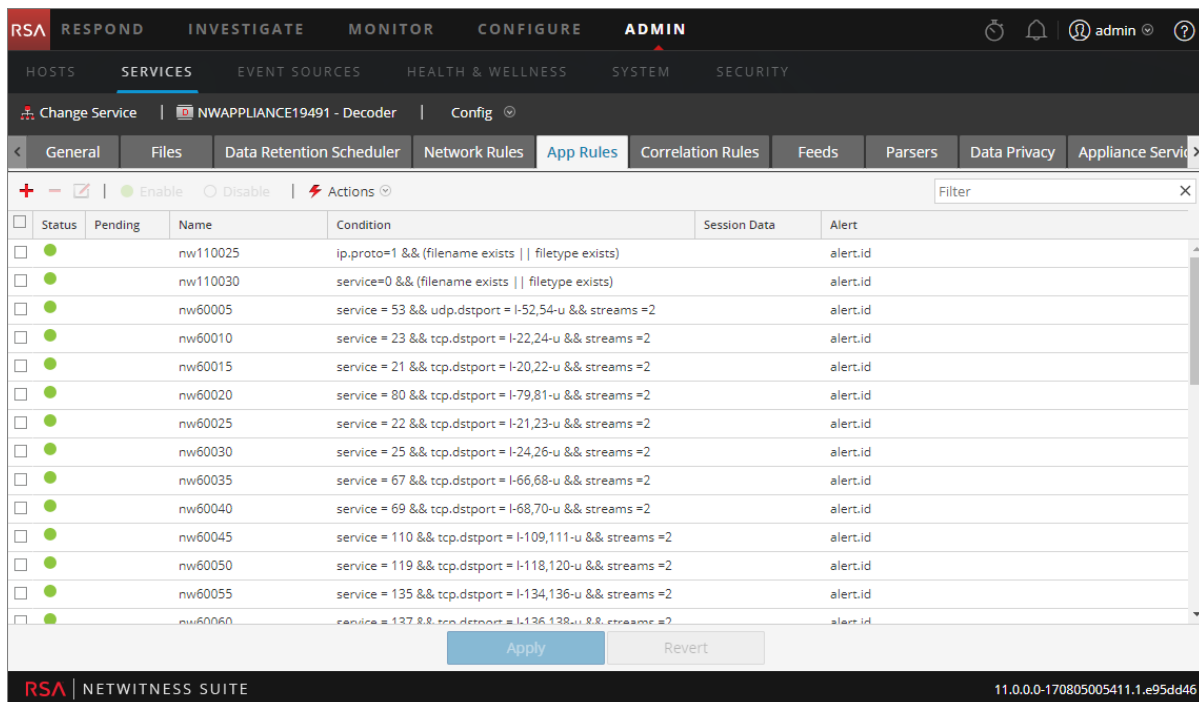
User Role	I want to...	Documentation
Administrator	add or edit application rules	<a href="#">Configure Application Rules</a>

### Related Topics


- [Decoder and Log Decoder Quick Setup](#)
- [Configure Common Settings on a Decoder](#)
- [Configure Decoder Rules](#)
- [Services Config View - Rules Tabs](#)

### Quick Look

The following figure shows an App Rules tab and the table describes the columns..

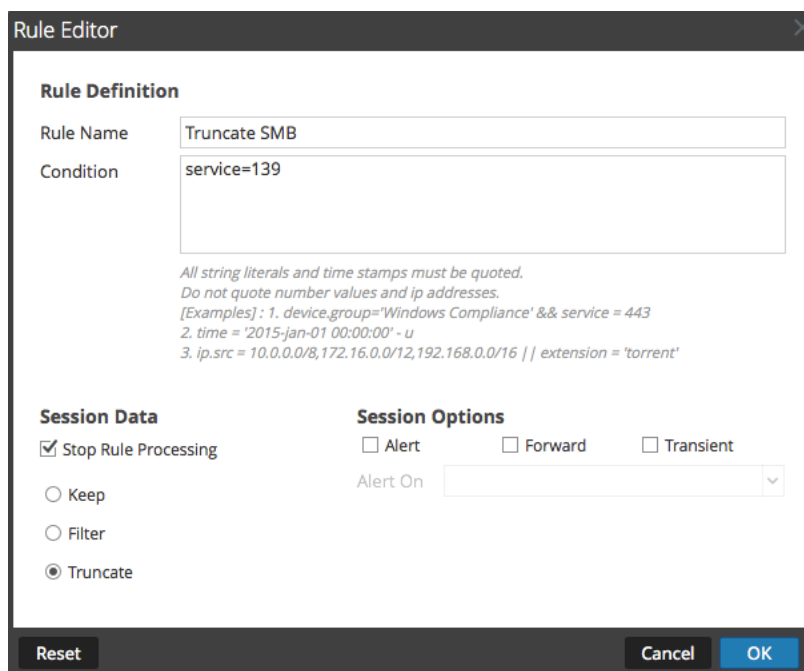


Status	Pending	Name	Condition	Session Data	Alert
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw110025	ip.proto=1 && (filename exists    filetype exists)		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw110030	service=0 && (filename exists    filetype exists)		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60005	service = 53 && udp.dstport = I-52,54-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60010	service = 23 && tcp.dstport = I-22,24-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60015	service = 21 && tcp.dstport = I-20,22-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60020	service = 80 && tcp.dstport = I-79,81-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60025	service = 22 && tcp.dstport = I-21,23-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60030	service = 25 && tcp.dstport = I-24,26-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60035	service = 67 && tcp.dstport = I-66,68-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60040	service = 69 && tcp.dstport = I-68,70-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60045	service = 110 && tcp.dstport = I-109,111-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60050	service = 119 && tcp.dstport = I-118,120-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60055	service = 135 && tcp.dstport = I-134,136-u && streams =2		alert.id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	nw60060	service = 137 && tcp.dstport = I-136,138-u && streams =2		alert.id

Column	Description
<b>Pending</b>	This column indicates whether a rule has pending changes. Rules that are currently active on the Decoder have no indicator. If the rule is new or has been modified, the column contains  . Once the rules are applied, the pending indicator is removed.
<b>Name</b>	This is the rule name, a descriptive identifier for the rule.
<b>Condition</b>	This is the definition of the condition that triggers an action when matched.
<b>Session Data</b>	This column displays the Session Data action taken when a packet matches the rule. Possible values are <b>Filter</b> , <b>Keep</b> , or <b>Truncate</b> .
<b>Alert</b>	This column displays the name of the custom alert that the Decoder generates when metadata matches the rule.
<b>Status</b>	This column indicates whether the rule is enabled or disabled with a circle icon. If the circle is filled green, the rule is enabled. If the circle is empty, the rule is disabled.

### Rule Editor Dialog

The following figure shows the Rule Editor dialog for an application rule.



**Rule Editor**

**Rule Definition**

Rule Name: Truncate SMB

Condition: service=139

*All string literals and time stamps must be quoted.  
Do not quote number values and ip addresses.  
[Examples] : 1. device.group='Windows Compliance' && service = 443  
2. time = '2015-jan-01 00:00:00' - u  
3. ip.src = 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16 || extension = 'torrent'*

**Session Data**

☒ Stop Rule Processing

☐ Keep

☐ Filter

☒ Truncate

**Session Options**

☐ Alert ☐ Forward ☐ Transient

Alert On:

Reset Cancel OK

The Rule Editor dialog provides the fields and options needed to define an application rule.

Field	Description
<b>Rule Name</b>	The descriptive name that identifies the rule.
<b>Condition</b>	<p>The definition of the condition that triggers an action when matched. You can type directly in the field or build the condition in this field using meta from the Intellisense window actions. As you build the rule definition, Intellisense displays syntax errors and warnings.</p> <p>All string literals and time stamps must be quoted. Do not quote number values and IP addresses. <a href="#">Configure Decoder Rules</a> provides additional details.</p>


The following table describes the Session Data actions and options.

Action	Description
<b>Stop Rule Processing</b>	If checked, further rule evaluation ends if the rule is matched, and the session is saved in accordance with the session action. If not checked, rule evaluation continues until all rules are evaluated.
<b>Keep</b>	The packet payload and associated metadata are saved when they match the rule.
<b>Filter</b>	The packet is not saved when it matches the rule.
<b>Truncate</b>	The packet payload is not saved when it matches the rule, but packet headers and associated metadata are retained.
<b>Alert and Alert On</b>	If <b>Alert</b> is checked, the packet generates a custom alert when metadata matches the rule. You can select the name of the alert in the <b>Alert On</b> field.
<b>Forward</b>	Enables the performance of syslog forwarding when the log matches the rule.
<b>Transient</b>	Prevents the alert metadata that is created from being written to the disk.

The following table describes Rule Editor dialog actions.

Action	Description
<b>Reset</b>	Resets the contents of the dialog to their values before editing; changes are discarded.
<b>Cancel</b>	Cancels any edits and closes the Rule Editor dialog.
<b>OK</b>	Saves the new rule or edited rule, and adds it to the rules grid. The Rule Editor dialog closes.
<b>Save</b>	(Rules with deprecated syntax only) Applies a corrected rule individually to the Decoder service. See <a href="#">Fix Rules with Invalid Syntax</a> .

## Correlation Rules Tab

The Correlation Rules tab (**ADMIN > Services > select a service and click  > View > Config > Correlation Rules tab**) enables you to manage correlation rules. Basic correlation rules are applied at the session level and alert the user to specific activities that may be occurring in their environment. NetWitness Suite applies correlation rules over a configurable sliding time window.

### What do you want to do?

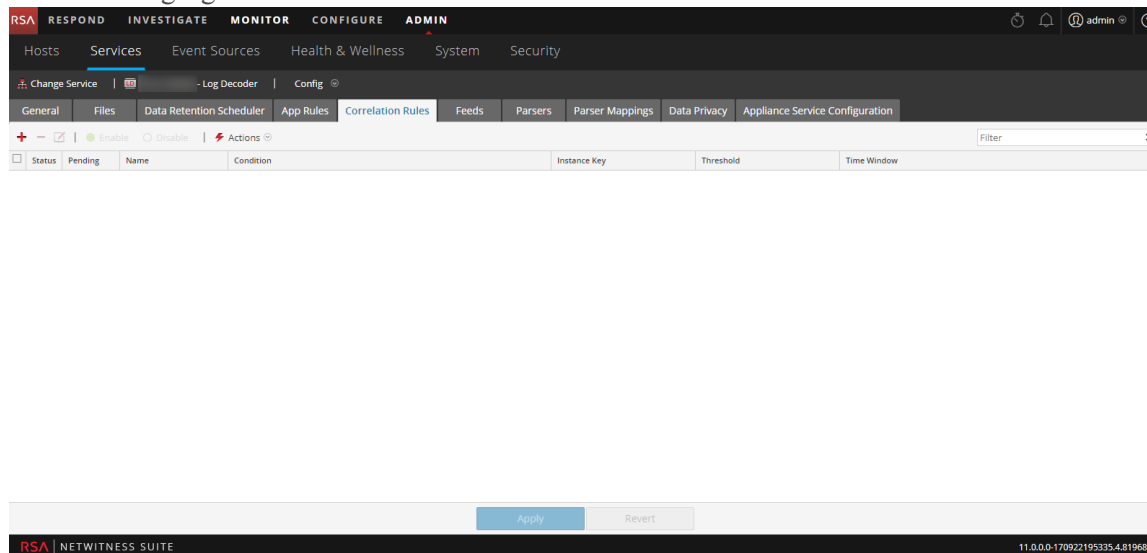
User Role	I want to...	Documentation
Administrator	add or edit a correlation rule	<a href="#">Configure Correlation Rules</a>

### Related Topics

- [Configure Common Settings on a Decoder](#)
- [Decoder and Log Decoder Quick Setup](#)
- [Configure Decoder Rules](#)
- [Services Config View - Rules Tabs](#)

### Quick Look

The following figure shows the Correlation Rules tab.



The following figure shows the Rule Editor dialog for a correlation rule.

**Rule Editor**

**Rule Definition**

Rule Name

Condition

**Correlation Fields**

Threshold

Instance Key

Time Window

**Reset** **Validate** **Cancel** **OK**

The following table describes the Correlation Rules tab columns.

Column	Description
<b>Pending</b>	This column indicates whether a rule has pending changes. Rules that are currently active on the Decoder have no indicator. If the rule is new or has been modified, the column contains . Once the rules are applied, the pending indicator is removed.
<b>Name</b>	This is the descriptive name for the rule.
<b>Condition</b>	<p>This is the definition of the condition that triggers an action when matched.</p> <p>In conditions, all string literals and time stamps must be quoted. Do not quote number values and IP addresses. <a href="#">Configure Decoder Rules</a> provides additional details.</p>
<b>Instance Key</b>	This is the target indicator to base the event upon. It can be a single primary key, such as ip.src or a compound primary key such as ip.src,ip.dst.





Column	Description
<b>Threshold</b>	<p>This is the minimum number of occurrences required to trigger a correlation session and can include a associated key that identifies the meta type that were are counting to determine if the condition is satisfied. The correlation engine cannot use IPv4 or IPv6 as an associated meta type. Use one of these three arguments:</p> <ul style="list-style-type: none"> <li>• <code>u_count(associated_key)</code> = the count of unique values of the specified key. A key is required.</li> <li>• <code>sum(associated_key)</code> = the values of the specified key. a key is required.</li> <li>• <code>count()</code> = number of sessions, no associated key used. If included, it is ignored.</li> </ul>
<b>Time Window</b>	This is the duration in hours, minutes, or seconds within which the threshold must be reached to trigger a correlation session.
<b>Status</b>	<p>This column indicates whether the rule is enabled or disabled with a circle icon. If the circle is filled green, the rule is enabled. If the circle is empty, the rule is disabled.</p>

The **Rule Editor** dialog provides the fields and options needed to define a network rule. The fields correspond exactly to the grid columns.

Action	Description
<b>Reset</b>	Resets the contents of the dialog to their values before editing; changes are discarded.
<b>Cancel</b>	Cancels any edits and closes the Rule Editor Dialog.
<b>OK</b>	Saves the new rule or edited rule, and adds it to the rules grid. The Rule Editor Dialog closes.
<b>Save</b>	(Rules with deprecated syntax only) Applies a corrected rule individually to the Decoder service. See <a href="#">Fix Rules with Invalid Syntax</a> .

## Network Rules Tab

The Network Rules tab (**ADMIN > Services > select a Decoder and click   > View > Config > Network Rules tab**) enables you to manage network rules. NetWitness Suite applies network rules at the packet level. Network rules consist of rule sets from Layer 2, Layer 3, and Layer 4. Multiple rules can be applied to the Decoder. Rules can be applied to multiple layers (for example, when a network rule filters out specific ports for a specific IP address). Network rules apply only to packet Decoders.

### What do you want to do?

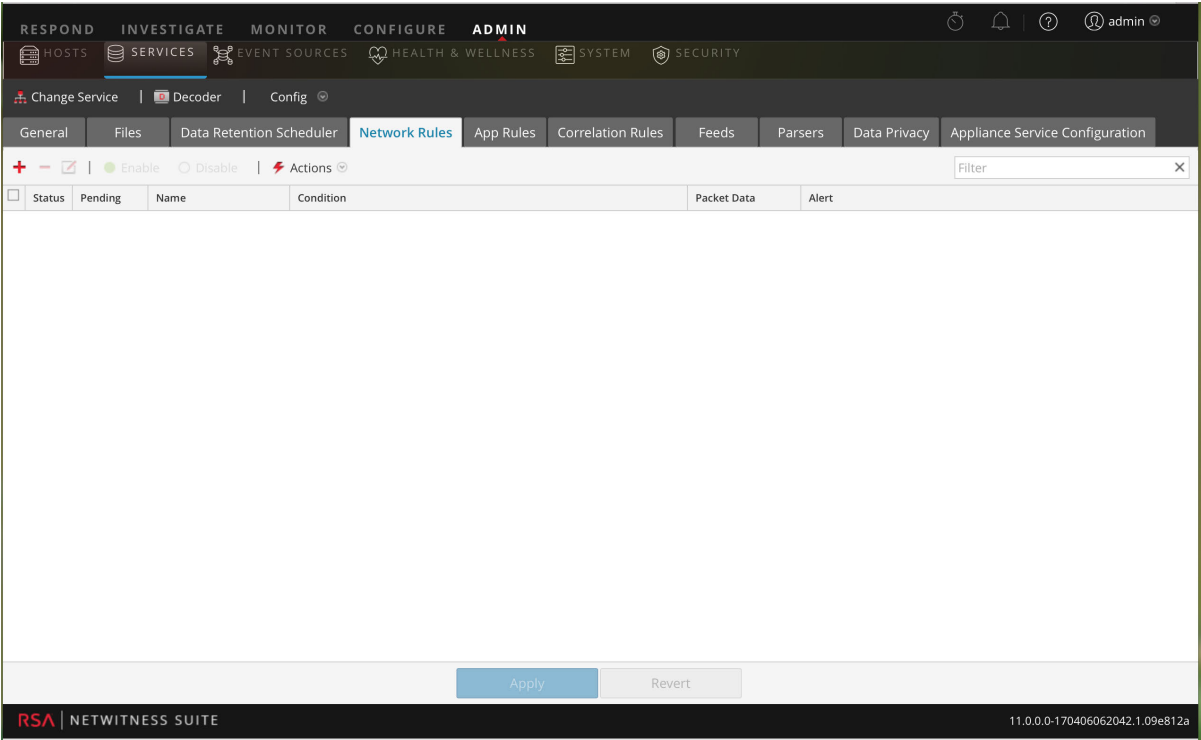
User Role	I want to...	Documentation
Administrator	add, edit, or fix network rules	<a href="#">Configure Network Rules</a>

### Related Topics

- [Decoder and Log Decoder Quick Setup](#)
- [Configure Common Settings on a Decoder](#)
- [Configure Decoder Rules](#)
- [Services Config View - Rules Tabs](#)

### Quick Look

The following figure shows the Network Rules tab.



The following figure shows the Rule Editor dialog for a network rule.

Rule Editor

Rule Definition

Rule Name

Subnet Filter

Condition

ip.addr=192.168.2.0/24

*All string literals and time stamps must be quoted.  
Do not quote number values and ip addresses.  
Examples : 1. ip.src = 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16  
2. tcp.srcport= 20,21,22,80*

Session Data

☒ Stop Rule Processing  
☐ Keep  
☒ Filter  
☐ Truncate

Session Options


☐ Assemble  
☐ Application Meta  
☐ Network Meta  
☐ Alert

Reset

Cancel

OK

The following table describes the columns in the Network Rules grid.

Column	Description
<b>Pending</b>	This column indicates whether a rule has pending changes. Rules that are currently active on the Decoder have no indicator. If the rule is new or has been modified, the column contains  . Once the rules are applied, the pending indicator is removed.
<b>Name</b>	This is the rule name, a descriptive identifier for the rule.
<b>Condition</b>	This is the definition of the condition that triggers an action when matched.
<b>Packet Data</b>	This column displays the Session Data action taken when a packet matches the rule. Possible values are <b>Filter</b> , <b>Keep</b> , or <b>Truncate</b> .

Column	Description
<b>Alert</b>	This column indicates whether the Decoder generates a custom alert when metadata matches the rule. Possible values are <b>Enabled</b> or <b>Disabled</b> .
<b>Status</b>	This column indicates whether the rule is enabled or disabled with a circle icon. If the circle is filled green, the rule is enabled. If the circle is empty, the rule is disabled.

The **Rule Editor** dialog provides the fields and options needed to define a network rule.

The following table describes the Rule Definition fields.

Field	Description
<b>Rule Name</b>	The descriptive name that identifies the rule.
<b>Condition</b>	<p>The definition of the condition that triggers an action when matched. You can type directly in the field or build the condition in this field using meta from the Intellisense window actions. As you build the rule definition, Intellisense displays syntax errors and warnings.</p> <p>In conditions, all string literals and time stamps must be quoted. Do not quote number values and IP addresses. <a href="#">Configure Decoder Rules</a> provides additional details. This section also describes the meta keys that NetWitness Suite supports for use in network rule conditions.</p>

The following table describes the Session Data actions.

Action	Description
<b>Stop Rule Processing</b>	If checked, further rule evaluation ends if the rule is matched, and the session is saved as indicated. If not checked, rule evaluation continues until all rules are evaluated.

Action	Description
<b>Keep</b>	The packet payload and associated meta are saved when they match the rule.
<b>Filter</b>	The packet is not saved when it matches the rule.
<b>Truncate</b>	The packet payload is not saved when it matches the rule, but packet headers and associated meta are retained.

The following table describes the session options.

Action	Description
<b>Assemble</b>	If checked, the assembler assembles the packet chain when it matches the rule.
<b>Network Meta</b>	The packet generates network metadata when it matches the rule.
<b>Application Meta</b>	The packet generates application metadata when it matches the rule.
<b>Alert</b>	The packet generates a custom alert when metadata matches the rule.

The following table describes Rule Editor dialog actions.

Action	Description
<b>Reset</b>	Resets the contents of the dialog to their values before editing; changes are discarded.
<b>Cancel</b>	Cancels any edits and closes the Rule Editor dialog.
<b>OK</b>	Saves the new rule or edited rule, and adds it to the rules grid. The Rule Editor dialog closes.
<b>Save</b>	(Rules with deprecated syntax only) Applies a corrected rule individually to the Decoder service. See <a href="#">Fix Rules with Invalid Syntax</a> .

## Services System View - Decoders

A Log Decoder is a special type of Decoder, and is configured and managed in a similar way to a Decoder. Therefore, most of the information in this section refers to both types of Decoders. Differences for Log Decoders are noted.

To reach the Services System view, go to **ADMIN > Services** > select a Decoder or Log Decoder >  > **View > System**.

### Workflow

The following figure depicts the workflow for common Decoder configuration tasks with the steps you can complete in this view highlighted.



### What do you want to do?

User Role	I want to...	Documentation
Administrator	configure capture settings	<a href="#">Configure Capture Settings</a>
Administrator	manage parsers and log parsers	<a href="#">Enable and Disable Parsers and Log Parsers</a>
Administrator	start and stop data capture*	<a href="#">Start and Stop Data Capture</a>
Administrator	upload packet capture and log files*	<a href="#">Upload a Log File to a Log Decoder</a> <a href="#">Upload a Packet Capture File</a>
Administrator	reset log stats, perform host tasks, shutdown the service, shutdown the appliance service, and reboot the host*	<i>Hosts and Services Getting Started Guide</i>

User Role	I want to...	Documentation
Administrator	configure rules	<a href="#">Configure Decoder Rules</a>

\*You can complete these tasks here.

## Related Topics

Go to the [Master Table of Contents](#) for Version 11.0 to find NetWitness Suite 11.0 documents.

- [Decoder and Log Decoder Quick Setup](#)
- [Configure Common Settings on a Decoder](#)
- "Services System View" in the *Hosts and Services Getting Started Guide*

## Quick Look

This is an example of the Services System view for a Decoder.

**Decoder Service Information**

Name	[REDACTED] (Decoder)
Version	11.0.0.0 (Rev null)
Memory Usage	249 MB (0.78% of 32176 MB)
CPU	1%
Running Since	2017-Sep-07 09:53:56
Uptime	6 days 23 hours 26 minutes 31 seconds
Current Time	2017-Sep-14 09:20:27

**Appliance Service Information**

Name	[REDACTED]
Version	11.0.0.0 (Rev null)
Memory Usage	23908 KB (0.07% of 32176 MB)
CPU	2%
Running Since	2017-Sep-07 07:10:51
Uptime	1 week 2 hours 9 minutes 36 seconds
Current Time	2017-Sep-14 09:20:27

**Decoder User Information**

Name	admin
Groups	Administrators
Roles	aggregate, connections.manage, database.manage, decoder.manage, dpo.manage, index.manage, logs.manage, parsers.manage, rules.manage, sdk.content, sdk.manage, sdk.meta, sdk.packets, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

**Host User Information**

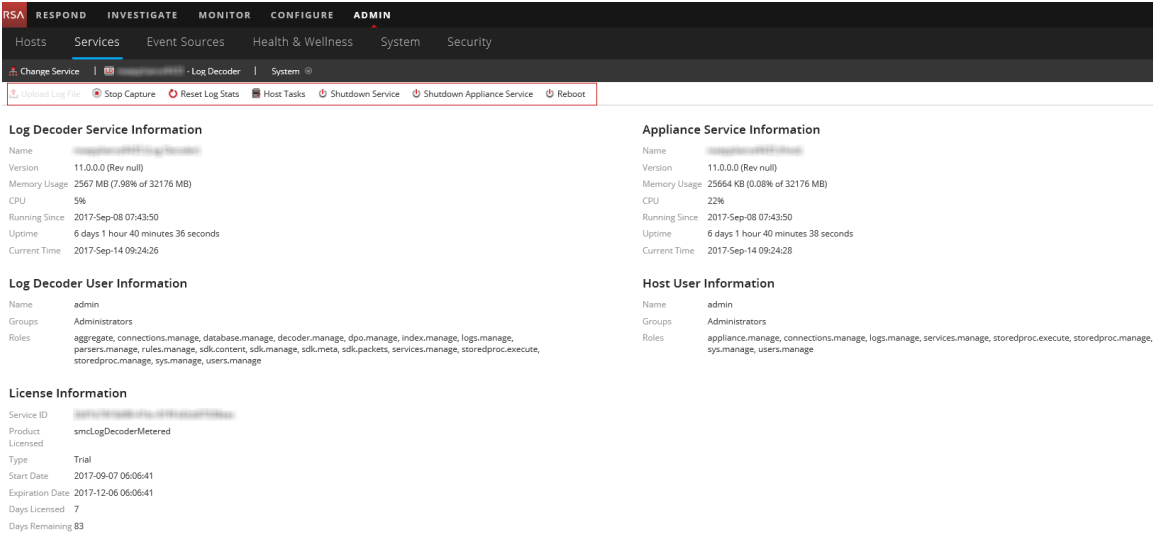
Name	admin
Groups	Administrators
Roles	appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

**License Information**

Service ID	[REDACTED]
Product	smcDecoderMetered
Licensed	
Type	Trial
Start Date	2017-09-07 06:06:41
Expiration Date	2017-12-06 06:06:41
Days Licensed	7
Days Remaining	83

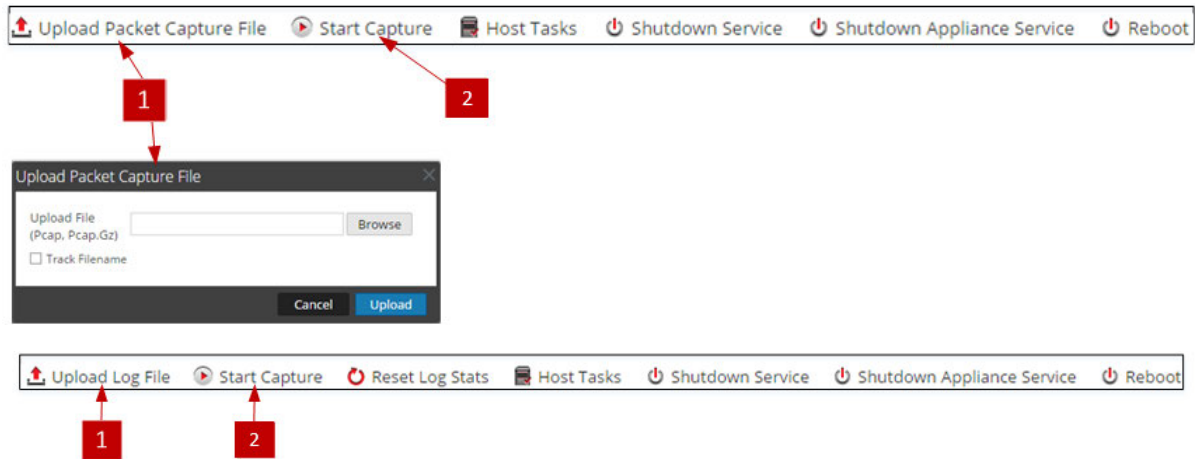
This is an example of the Services System view for a Log Decoder.





### Service Info Toolbar

These two toolbars illustrate the options specific to Decoders and Log Decoders.



In addition to the common options in the Services System view toolbar, you can start and stop capture of packets or logs. The upload file options are different for the standard Decoder (packet capture file) and the Log Decoder (log file).

Action	Description
Upload Packet Capture File	Displays a dialog that provides a way to select a packet capture (.pcap) file for upload to the selected Decoder. For more information, see <a href="#">Upload a Packet Capture File</a> .
	<b>Note:</b> This option does not apply to Log Decoders.

Action	Description
<b>Upload Log File</b>	Displays a dialog that provides a way to select a log (.log) file for upload to the selected Log Decoder. For more information, see <a href="#">Upload a Log File to a Log Decoder</a> .
<b>Start/Stop Capture</b>	Starts packet capture on the selected Decoder. When packet capture is in progress, the option in the toolbar changes to Stop Capture, and the option to upload a file is unavailable.

