



# System Configuration Guide

for Version 11.0



Copyright © 1994-2017 Dell Inc. or its subsidiaries. All Rights Reserved.

## **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.

February 2018

# Contents

---

<b>System Configuration Overview</b> .....	<b>6</b>
<b>Standard Procedures</b> .....	<b>7</b>
Access System Settings .....	8
Configure Notification Servers .....	9
Notification Servers Overview .....	9
Configure the Email Settings as Notification Server .....	10
Configure Script as a Notification Server .....	11
Configure the SNMP Settings as Notification Server .....	12
Configure a Syslog Notification Server .....	13
Configure Notification Outputs .....	15
Notification Outputs Overview .....	15
Configure Email as a Notification .....	16
Configure Script as a Notification .....	17
Configure SNMP as a Notification .....	18
Configure Syslog as a Notification .....	19
Configure Templates for Notifications .....	21
Configure Global Notifications Templates .....	21
Define a Template for ESA Alert Notifications .....	24
Import and Export a Global Notifications Template .....	26
Configure Email Servers and Notification Accounts .....	27
Configure Global Audit Logging .....	30
Global Audit Logging - High-Level Procedure .....	31
Configure a Destination to Receive Global Audit Logs .....	33
Define a Template for Global Audit Logging .....	37
Define a Global Audit Logging Configuration .....	42
Verify Global Audit Logs .....	45
Configure Investigation Settings .....	48
Configure Navigate, Events, and Context Lookup Settings .....	48
Clear Reconstruction Cache for Services .....	50
Configure Live Services Settings .....	52
About Live Feedback Participation .....	53

---

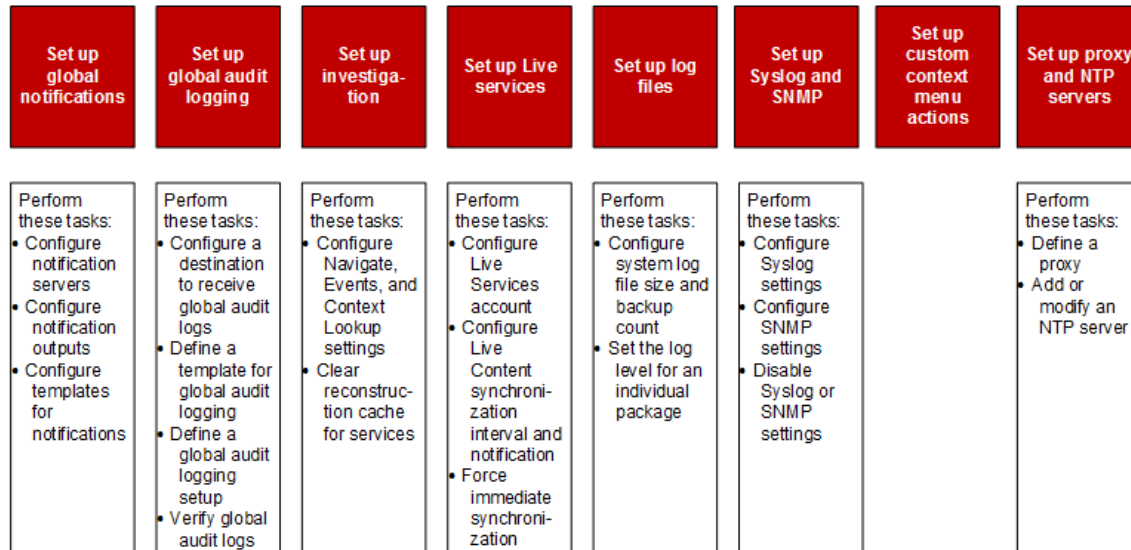
Live Feedback Overview .....	58
Upload Data to RSA for Live Feedback .....	67
Configure Log File Settings .....	68
Configure System Log File Size and Backup Count .....	68
Set the Log Level for an Individual Package .....	69
Configure Syslog and SNMP Settings .....	70
Configure and Enable Syslog Settings .....	70
Configure and Enable SNMP Settings .....	71
Disable Syslog or SNMP Settings .....	72
<b>Additional Procedures .....</b>	<b>73</b>
Add Custom Context Menu Actions .....	73
Example Procedure: Context Menu Action to Investigate ip.dst from alias.ip .....	77
Configure NTP Servers .....	79
Add an NTP Server .....	80
Modify an NTP Server .....	81
Add New Configuration Dialog .....	83
User Actions Logged .....	84
<b>Troubleshooting System Configuration .....</b>	<b>87</b>
Troubleshoot Global Audit Logging .....	87
Advanced Troubleshooting .....	88
Troubleshooting NTP Server Configuration .....	97
Issues Identified by Messages in the NTP Settings Panel or Log Files .....	97
<b>References .....</b>	<b>99</b>
Global Audit Logging Configurations Panel .....	100
Global Notifications Panel .....	104
Define Notification Server Dialogs .....	109
Define Notification Output Dialogs .....	120
Define Notification Template Dialog .....	126
Output Tab .....	129
Servers Tab .....	132
Templates Tab .....	135
HTTP Proxy Settings Panel .....	137
Email Configuration Panel .....	139
ESA Settings Panel .....	142
Investigation Configuration Panel .....	144

---

Live Services Configuration Panel .....	155
About Live Feedback Participation .....	164
NTP Settings Panel .....	165
Context Menu Actions Panel .....	168
Legacy Notifications Configuration Panel .....	174
Supported CEF Meta Keys .....	178
Supported Common Event Format (CEF) Meta Keys .....	178
Supported Global Audit Logging Meta Key Variables .....	185
Supported Global Audit Logging Meta Key Variables .....	185
Global Audit Logging Operation Reference .....	187
CARLOS .....	187
ESA .....	188
Investigation .....	189
Reporting Engine .....	192
Warehouse Connector .....	194
Health & Wellness .....	195
NetWitness Suite Core Services .....	195
Malware Analysis .....	201
NetWitness Suite User Interface .....	205
Respond .....	210
Local Audit Log Locations .....	212

## System Configuration Overview

In the Administration System view, administrators can configure system settings to receive optimal performance from NetWitness Suite. This diagram shows the available configuration options.



In this guide, the standard procedures provide instructions for administrators who want to customize settings that apply across the system in NetWitness Suite. Although some of these settings have default values, the administrator needs to view and evaluate all default values.

Additional procedures are not essential for the set up of NetWitness Suite, they include certain customization options that are beyond the usual setup; for example, adding custom context menus or setting up a proxy.

In addition, reference topics and troubleshooting topics supply detailed information about the user interface and suggestions for resolving possible issues.

The following sections describe system configuration:

- [Standard Procedures](#) provide instructions for administrators who want to customize settings that apply across the system in NetWitness Suite.
- [Additional Procedures](#) provide instructions for setting up customization options that are beyond the usual system configuration.

## Standard Procedures

---

The topics in this section provide instructions for administrators who want to customize settings that apply across the system in NetWitness Suite. Although some of these settings have default values, the administrator needs to view and evaluate all default values. The procedures can be performed in any sequence and are listed alphabetically.

[Access System Settings](#)

[Configure Notification Servers](#)

[Configure Notification Outputs](#)

[Configure Templates for Notifications](#)

[Configure the Email Settings as Notification Server](#)

[Configure Email Servers and Notification Accounts](#)

[Configure Global Audit Logging](#)

[Configure Investigation Settings](#)

[Configure Live Services Settings](#)

[Configure Log File Settings](#)

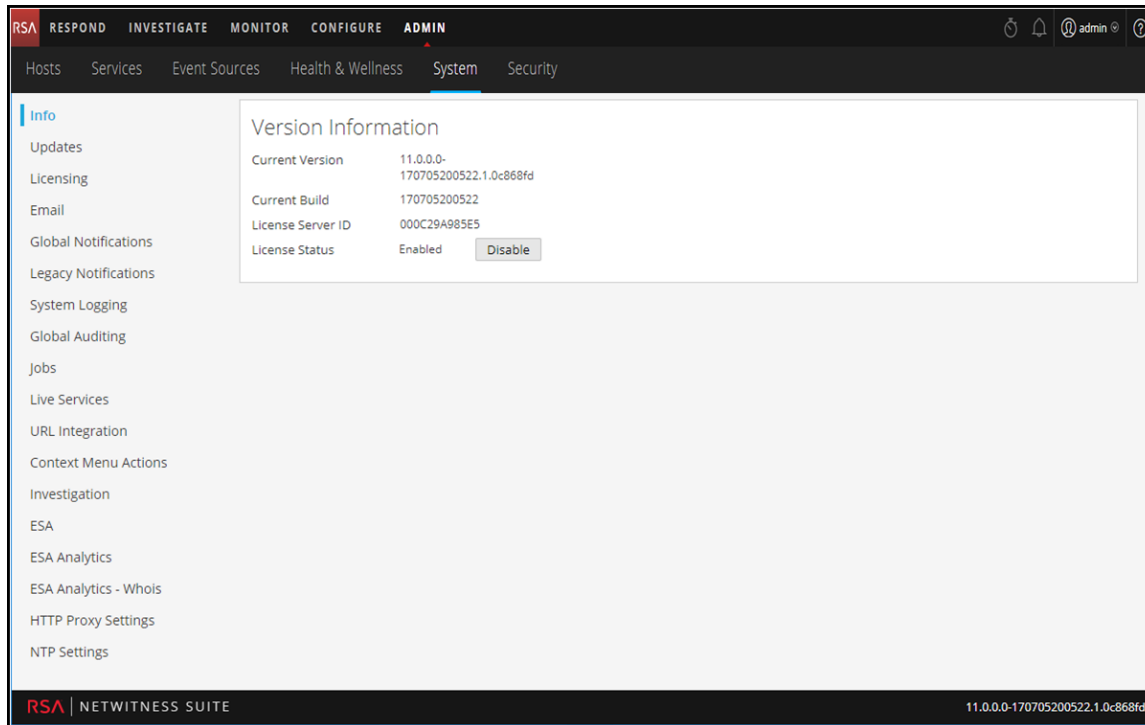
## Access System Settings

This topic introduces system configuration capabilities of NetWitness Suite in the Administration System view. Administrators can configure notifications, email notifications, global audit logging, logging settings, connection to Live Services, and URL integration in NetWitness Suite.

To access the system settings:

Go to **ADMIN > System**.

The Administration System view is displayed.



On the left panel of the Administration System view is an options panel listing all system nodes available for configuration. When you select a node, the associated content is displayed in the right panel.



## Configure Notification Servers

This topic provides instructions on how to configure notification servers. For ESA, notification servers are required to define an ESA rule. A notification server is also required to configure global audit logging.

Global Notifications configurations define notifications settings for Event Source Management (ESM), Health and Wellness, Global Audit Logging, Event Stream Analysis (ESA), and Respond. Notification Servers define the servers from which you want to receive notifications from the system. For Global Audit Logging, define Log Decoders as Syslog Notification Servers.

You can define, delete, edit, import, and export a notification server in NetWitness Suite. Individual topics describe the relevant procedures. For more information on ESA alert configuration, see "Notification Methods" in the *Alerting Using ESA Guide*. You delete, edit, import, and export notification outputs and notification servers in the same way as templates. You cannot disable or delete notification servers associated with global audit logging configurations.

### Notification Servers Overview

This topic provides an overview of notification servers. You configure notification servers in the Administration System view (ADMIN > System > Notifications > Servers tab).

Global Notifications are used by a variety of components in NetWitness Suite, such as Event Stream Analysis (ESA), Respond, Health and Wellness, Event Source Management (ESM), and Global Audit Logging. Notification settings are called **Notification Servers**.

Event Stream Analysis sends notifications to users through email, SNMP, or Syslog about various system events. In ESA, these alert notification settings are called Notification Servers. You can configure multiple notification servers and use them while defining an ESA rule, for example, you can configure multiple mail servers or Syslog servers and use the settings while defining an ESA rule.

You can configure the following notification servers:

- Email
- SNMP
- Syslog
- Script

Email notification servers enable you to configure email server settings to send alert notifications. SNMP notification servers enable you to configure SNMP trap host settings as a notification server to send alert notifications.

Syslog notification servers enable you to configure Syslog settings as a notification server to send notifications. When enabled, Syslog provides auditing through the use of the RFC 5424 Syslog protocol. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis. For Global Audit Logging, you can only use Syslog Notification Servers.

Script notification servers enable you to configure Script as a notification server.

For detailed information on the different notification server configurations, including parameters and descriptions, see [Define Notification Server Dialogs](#).

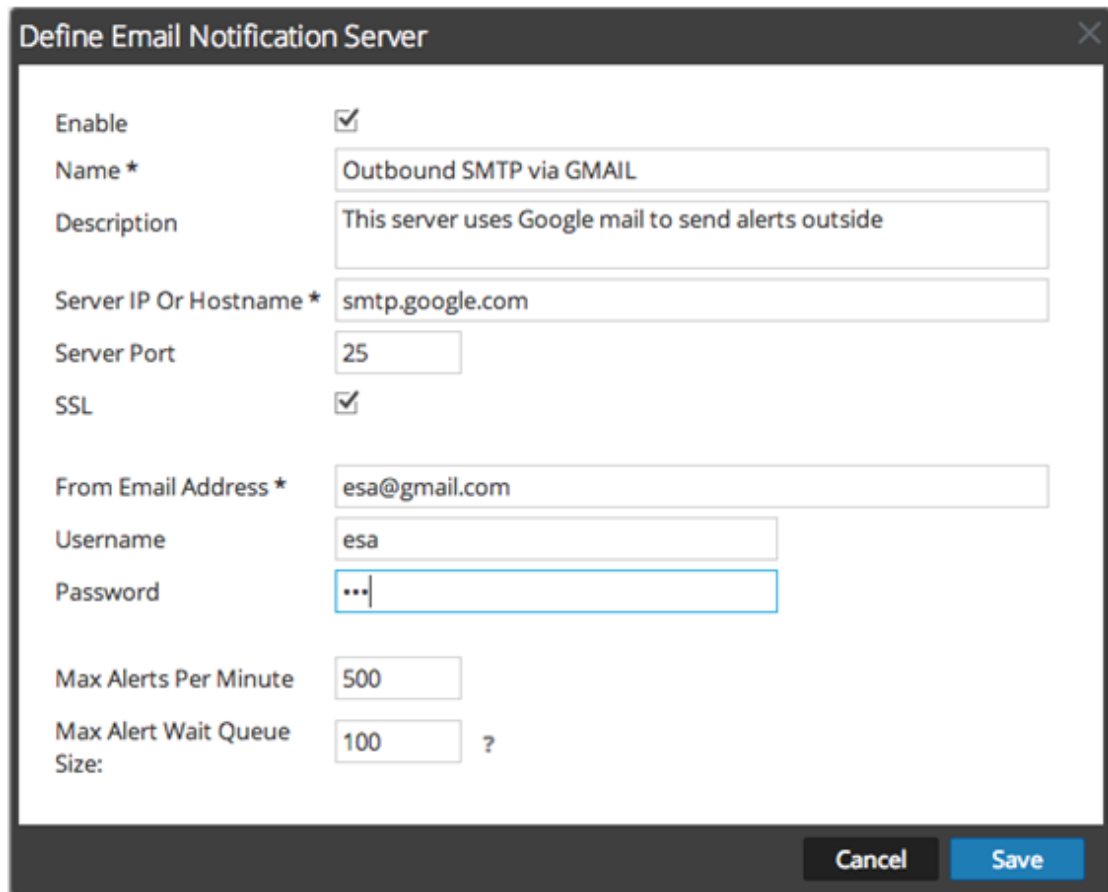
## Configure the Email Settings as Notification Server

To configure email server settings as a notification server to send alert notifications:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.  
The **Notifications** configuration panel is displayed with the **Output** tab open.
3. Click the **Servers** tab.

Enable	Name	Output	Description	Last Modified	Actions
<input type="checkbox"/>	● Email-Cica	Email		2017-09-20 05:33:30	⚙️
<input type="checkbox"/>	● Email-Rachana	Email		2017-09-20 10:35:14	⚙️
<input type="checkbox"/>	● SNMP	SNMP		2017-09-20 10:51:56	⚙️
<input type="checkbox"/>	● Syslog	Syslog		2017-09-20 18:41:03	⚙️

- From the   drop-down menu, select **Email**.



**Define Email Notification Server**

Enable

Name \* Outbound SMTP via GMAIL

Description This server uses Google mail to send alerts outside

Server IP Or Hostname \* smtp.google.com

Server Port 25

SSL

From Email Address \* esa@gmail.com

Username esa

Password ...

Max Alerts Per Minute 500

Max Alert Wait Queue Size: 100 ?

Cancel Save

- In the **Define Email Notification Server** dialog, provide the required information and click **Save**.

**Note:** For ESM/SMS and ESA notifications, you must specify only the hostname/FQDN in the Server IP or Hostname field.

For details of the parameters and descriptions, see [Define Notification Server Dialogs](#) .

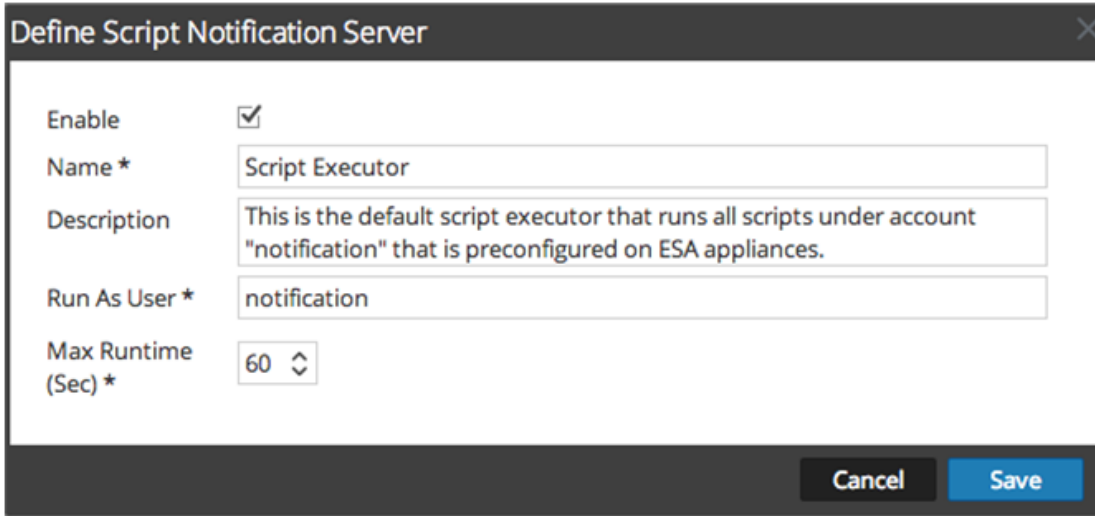
## Configure Script as a Notification Server

ESA allows you to run scripts in response to ESA alerts. However, you must first configure the user identity and other details that are required to run the scripts.

To configure Script as a notification server:

- Go to **ADMIN > System**.
- In the options panel, select **Global Notifications**.
- Click the **Servers** tab.

- From the   drop-down menu, select **Script**.



The image shows a dialog box titled "Define Script Notification Server" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Enable:** A checked checkbox.
- Name \*:** A text input field containing "Script Executor".
- Description:** A text area containing "This is the default script executor that runs all scripts under account 'notification' that is preconfigured on ESA appliances."
- Run As User \*:** A text input field containing "notification".
- Max Runtime (Sec) \*:** A spinner control set to "60".

At the bottom right of the dialog are two buttons: "Cancel" and "Save".

- In the **Define Script Notification Server** dialog, provide the required information and click **Save**.

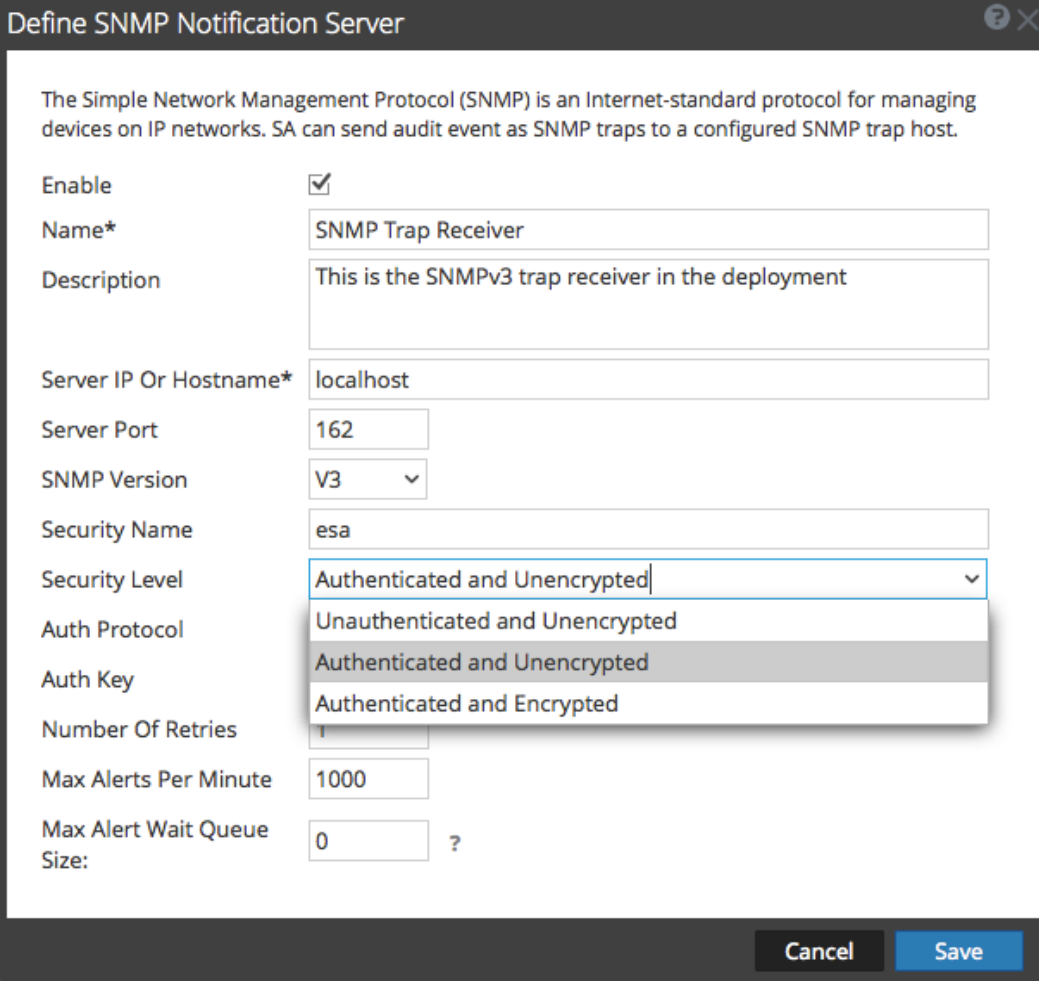
For details of the parameters and descriptions, see [Define Notification Server Dialogs](#).

## Configure the SNMP Settings as Notification Server

To configure the SNMP trap host settings as a notification server to send alert notifications:

- Go to **ADMIN > System**.
- In the options panel, select **Global Notifications**.
- Click the **Servers** tab.

4. From the   drop-down menu, select **SNMP**.



**Define SNMP Notification Server**

The Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. SA can send audit event as SNMP traps to a configured SNMP trap host.

Enable

Name\*

Description

Server IP Or Hostname\*

Server Port

SNMP Version

Security Name

Security Level

Auth Protocol

Auth Key

Number Of Retries

Max Alerts Per Minute

Max Alert Wait Queue Size:  ?

Cancel Save

5. In the **Define SNMP Notification Server** dialog, provide the required information and click **Save**.



For details of the parameters and descriptions, see [Define Notification Server Dialogs](#).

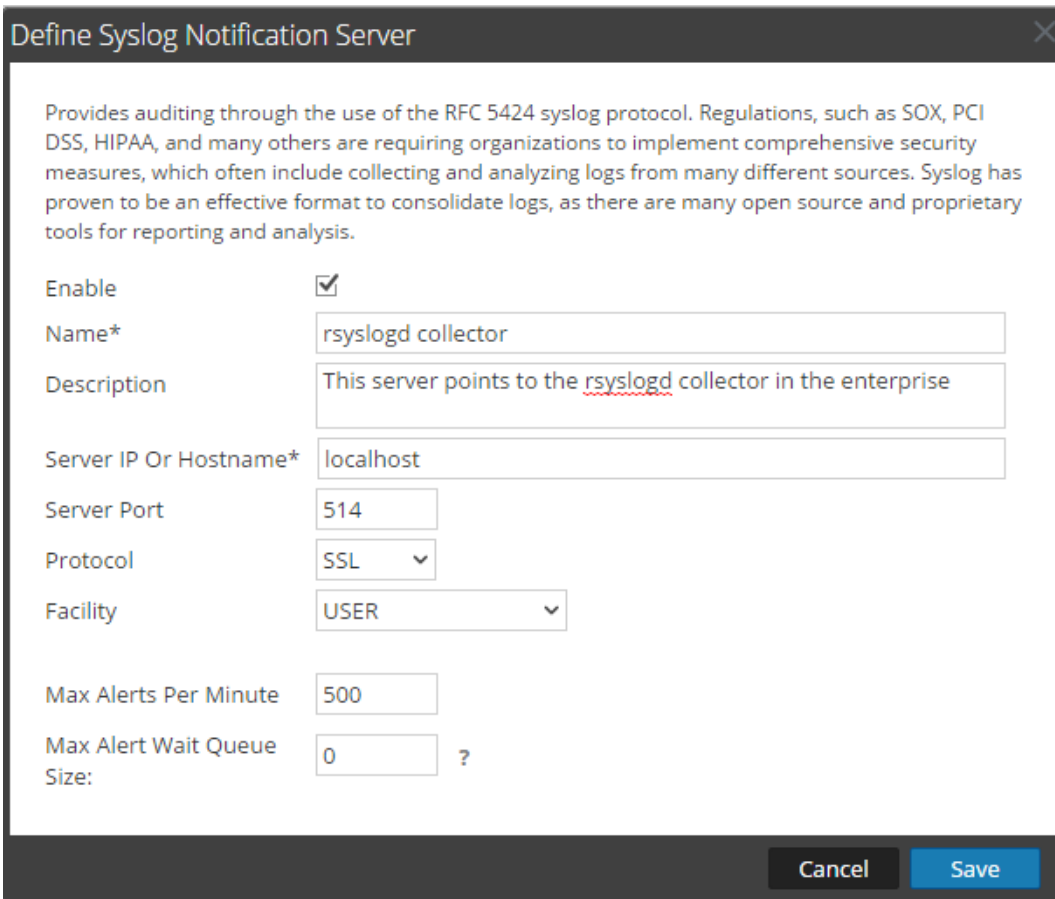
## Configure a Syslog Notification Server

This topic provides instructions on how to configure a Syslog notification server. When enabled, Syslog provides auditing through the use of the RFC 5424 Syslog protocol. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis.

To configure Syslog as a notification server:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.

3. Click the **Servers** tab.
4. From the   drop-down menu, select **Syslog**.



**Define Syslog Notification Server**

Provides auditing through the use of the RFC 5424 syslog protocol. Regulations, such as SOX, PCI DSS, HIPAA, and many others are requiring organizations to implement comprehensive security measures, which often include collecting and analyzing logs from many different sources. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis.

Enable

Name\*

Description

Server IP Or Hostname\*

Server Port

Protocol

Facility

Max Alerts Per Minute

Max Alert Wait Queue Size:  ?

5. In the **Define Syslog Notification Server** dialog, provide the required information and click **Save**.

For details of the parameters and descriptions, see [Define Notification Server Dialogs](#).

## Configure Notification Outputs

This topic provides instructions on how to configure notification outputs. These notification outputs are required to define an ESA rule.

Global Notifications configurations define notification settings for Event Source Management (ESM), Health and Wellness, Global Audit Logging, Event Stream Analysis (ESA), and Respond.

**Note:** You do not need to configure the Output tab for Global Audit Logging.

Notification Output configurations define email addresses and subject lines, SNMP trap OID settings, syslog output settings, and script code.

You can define, delete, edit, import, and export notification outputs in NetWitness Suite. Individual topics describe the relevant procedures. For more information on ESA alert configuration, see "Notification Methods." You delete, edit, import, and export notification outputs and notification servers in the same way as templates. If you attempt to delete a notification output being used by alerts, you will receive a warning confirmation message that the alerts using the notification will not function properly. The message shows the number of alerts in use.

### Notification Outputs Overview

This topic provides an overview of notification outputs. These notification outputs are required when defining an ESA rule. You configure notification outputs in the Administration System view (Administration > System > Notifications > Outputs tab).

Global Notifications configurations define notification settings for Event Source Management (ESM), Health and Wellness, Global Audit Logging, Event Stream Analysis (ESA), and Respond.

**Note:** You do not need to configure notification outputs (the Output tab) for Global Audit Logging.

Notification outputs are the destinations used for sending notifications. For ESA, notification outputs enable you to define how you want to receive the ESA alerts. The following are the different notification outputs supported by NetWitness Suite:

- Email
- SNMP
- Syslog
- Script

Email notification settings define the destination email address to which you can send the alerts. You can also add a custom description in the subject of the email and define multiple destination email addresses.

SNMP notification settings enable you to define the SNMP settings to send alert notifications. Syslog notifications enable you to define the Syslog settings used to send alert notifications. Script notifications enable you to define the Script that executes in response to the alert.

For detailed information on the notification configurations, including parameters and descriptions, see [Define Notification Server Dialogs](#).

## Configure Email as a Notification

To configure Email as a notification:

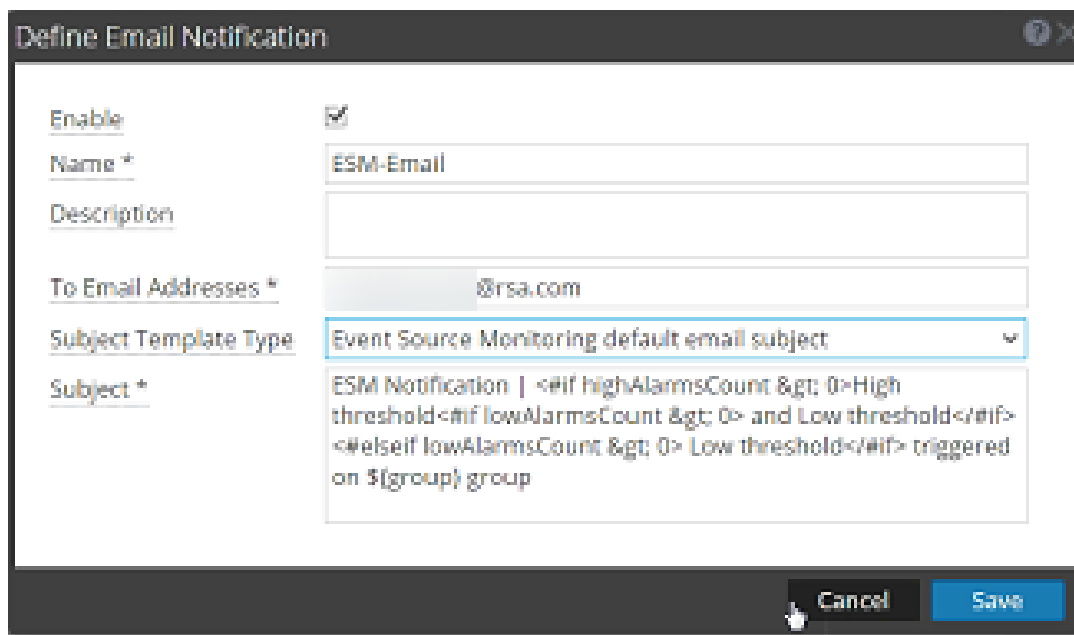
1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.

The screenshot shows the RSA NetWitness Suite Admin console. The top navigation bar includes 'RSA', 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The 'ADMIN' section is expanded to show 'System', which is selected. The left sidebar contains various configuration categories, with 'Global Notifications' highlighted. The main content area is titled 'Global Notifications' and has three tabs: 'Output', 'Servers', and 'Templates'. The 'Templates' tab is active, showing a table of notification templates. The table has columns for 'Name', 'Template Type', 'Description', and 'Actions'. The table lists 12 templates, including 'Default Audit CEF Template', 'Default Audit Human-Readable Format', 'Default SMTP Template', 'Default SNMP Template', 'Default Script Template', 'Default Syslog Template', 'ESM Default Email Template', 'ESM Default SNMP Template', 'ESM Default Syslog Template', 'Health & Wellness Default SMTP Template', and 'Health & Wellness Default SNMP Template'. The page also shows a search bar, a pagination control (Page 1 of 1), and a page size dropdown (25).

Name	Template Type	Description	Actions
<input type="checkbox"/> Default Audit CEF Template	Audit Logging	Default Audit CEF Template	
<input type="checkbox"/> Default Audit Human-Readable Format	Audit Logging	Default Audit Human-Readable Format	
<input type="checkbox"/> Default SMTP Template	Event Stream Analysis	Default SMTP Template	
<input type="checkbox"/> Default SNMP Template	Event Stream Analysis	Default SNMP Template	
<input type="checkbox"/> Default Script Template	Event Stream Analysis	System default FreeMarker template for Script notifications	
<input type="checkbox"/> Default Syslog Template	Event Stream Analysis	Default Syslog Template	
<input type="checkbox"/> ESM Default Email Template	Event Source Monitoring	ESM Default Email Template	
<input type="checkbox"/> ESM Default SNMP Template	Event Source Monitoring	ESM Default SNMP Template	
<input type="checkbox"/> ESM Default Syslog Template	Event Source Monitoring	ESM Default Syslog Template	
<input type="checkbox"/> Health & Wellness Default SMTP Template	Health Alarms	Health & Wellness Default SMTP Template	
<input type="checkbox"/> Health & Wellness Default SNMP Template	Health Alarms	Health & Wellness Default SNMP Template	



3. On the **Output** tab, from the   drop-down menu, select **Email**.



The image shows a dialog box titled "Define Email Notification". It contains the following fields and controls:

- Enable:** A checked checkbox.
- Name \*:** A text input field containing "ESM-Email".
- Description:** An empty text input field.
- To Email Addresses \*:** A text input field containing "@rsa.com".
- Subject Template Type:** A dropdown menu with the selected option "Event Source Monitoring default email subject".
- Subject \*:** A text input field containing the template: "ESM Notification | <#if highAlarmsCount > 0>High threshold<#if lowAlarmsCount > 0> and Low threshold</#if> <#elseif lowAlarmsCount > 0> Low threshold</#if> triggered on \$(group) group".

At the bottom right, there are two buttons: "Cancel" and "Save".

4. In the **Define Email Notification** dialog, provide the required information and click **Save**.  
For details of the parameters and descriptions, see [Define Notification Server Dialogs](#).

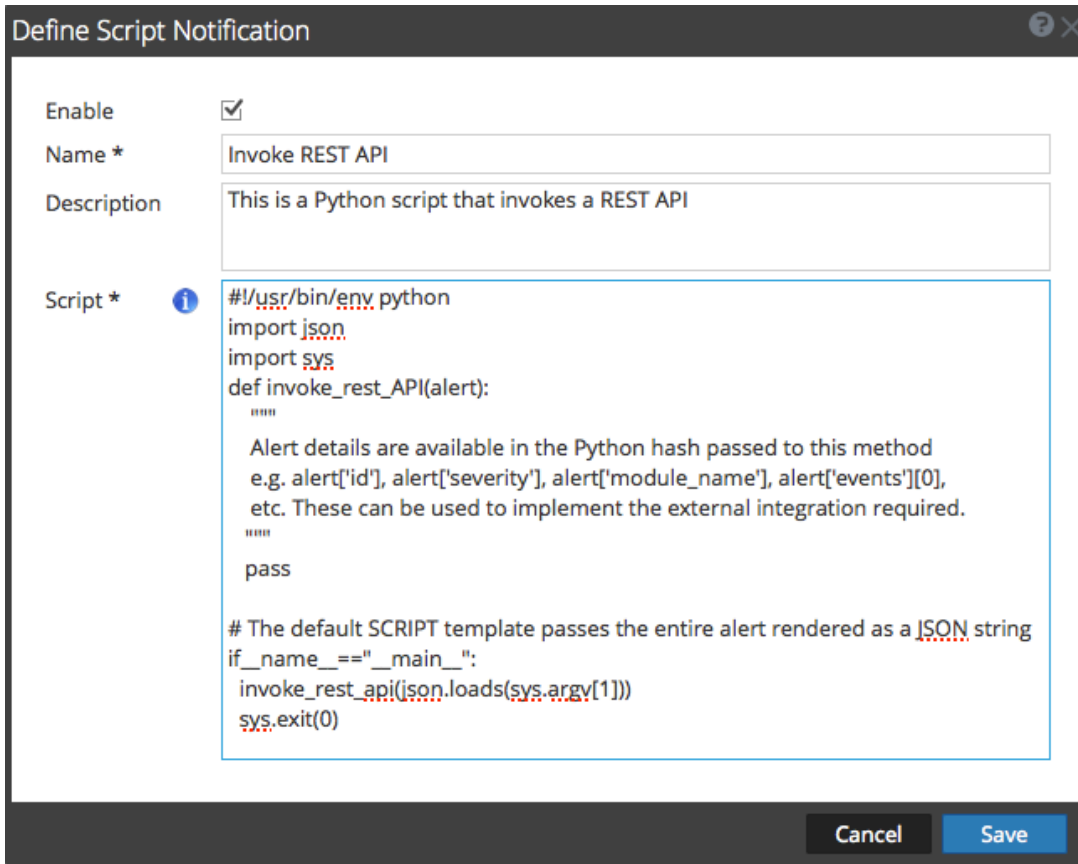
## Configure Script as a Notification

This topic provides instructions to define the Script and configure it as a notification output. ESA allows you to run scripts in response to ESA alerts. You need to define the script using the ADMIN > System > Notifications > Output tab. You can use any script for ESA notifications.

To configure the script as a notification:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.

- On the Output tab, from the   drop-down menu, select **Script**.



The image shows a dialog box titled "Define Script Notification". It has a dark header with a question mark and a close button. The dialog contains the following fields and content:

- Enable:** A checked checkbox.
- Name \*:** A text input field containing "Invoke REST API".
- Description:** A text input field containing "This is a Python script that invokes a REST API".
- Script \*:** A text area containing a Python script. The script starts with a shebang line and imports json and sys. It defines a function named invoke\_rest\_API that takes an alert as an argument. The function's docstring explains that alert details are available in the Python hash passed to the method. The function body is empty (pass). Below the function, there is a comment and a main block that calls invoke\_rest\_api with the first command-line argument and then exits.

At the bottom of the dialog, there are two buttons: "Cancel" and "Save".

- In the **Define Script Notification** dialog, provide the required information and click **Save**. For details of the parameters and descriptions, see [Define Notification Server Dialogs](#).

## Configure SNMP as a Notification

To configure SNMP as a notification output to send alert notifications:

- Go to **ADMIN > System**.
- In the options panel, select **Global Notifications**.

3. On the Output tab, from the   drop-down menu, select **SNMP**.

### Define SNMP Notification

The Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. NetWitness Suite can send audit event as SNMP traps to a configured SNMP trap host.


Enable

Name \*

Description

Trap OID

Message OID

Variables 

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>		

4. In the SNMP Notification dialog, provide the required information and click **Save**. For details of the parameters and descriptions, see [Define Notification Server Dialogs](#).

## Configure Syslog as a Notification


To configure Syslog as a notification output when sending alert notifications:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.

3. On the Output tab, from the   drop-down menu, select **Syslog**.

### Define Syslog Notification

Provides auditing through the use of the RFC 5424 syslog protocol. Regulations, such as SOX, PCI DSS, HIPAA, and many others are requiring organizations to implement comprehensive security measures, which often include collecting and analyzing logs from many different sources. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis.

Enable	<input checked="" type="checkbox"/>
Name *	<input type="text"/>
Description	<input type="text"/>
Severity	Informational 
Encoding	UTF-8
Max Length	2048
Include Local Timestamp	<input checked="" type="checkbox"/>
Include Local Hostname	<input checked="" type="checkbox"/>
Identity String	<input type="text"/>

4. In the **Define Syslog Notification** dialog, provide the required information and click **Save**. For details of the parameters and descriptions, see [Define Notification Server Dialogs](#).

## Configure Templates for Notifications

You configure notification templates in the Administration System view (ADMIN > System > Notifications > Templates tab). A notification template defines the format and message fields of the notifications. There are different template types for the notifications that you can configure:

- Audit Logging
- Event Stream Analysis
- Event Source Monitoring
- Health Alarms

You can use the available default templates or you can configure your own templates for Email, SNMP, Syslog, and Script, depending on the template type.

Global audit logging sends audit logs in the format specified in the Audit Logging template. You can use the default audit logging templates or you can define your own audit logging template. For more information on how to define an Audit Logging template, see [Define a Template for Global Audit Logging](#).

Event Stream Analysis (ESA) sends notifications in the format specified in the Event Stream Analysis templates. The default Event Stream Analysis templates for email, SNMP, Syslog, and Script are available on installation. You can customize these templates as well as create new templates which you can use for the notifications. For more information on how to define ESA templates, see [Define a Template for ESA Alert Notifications](#).

For more information on ESA alert configuration, see "Notification Methods" in the **Alerting Using ESA Guide**. You cannot delete templates associated with global audit log configurations.

**Note:** When upgrading from NetWitness Suite 10.4, all existing notification templates migrate to the Event Stream Analysis template type.

To learn how to define, delete, edit, duplicate, import, and export a notification template in NetWitness Suite, see:

[Configure Global Notifications Templates](#)

[Define a Template for ESA Alert Notifications](#)

[Import and Export a Global Notifications Template](#)

### Configure Global Notifications Templates

This topic provides instructions for adding, editing, duplicating, and deleting global notifications templates.

You can use the available default templates or you can configure your own templates for Email, SNMP, Syslog, and Script, depending on the template type.

Global audit logging sends audit logs in the format specified in the Audit Logging template. You can use the default audit logging templates or you can define your own audit logging template. For more information on how to define an Audit Logging template, see "Define a Template for Global Audit Logging."

Event Stream Analysis (ESA) sends notifications in the format specified in the Event Stream Analysis templates. The default Event Stream Analysis templates for email, SNMP, Syslog, and Script are available on installation. You can customize these templates as well as create new templates which you can use for the notifications. For more information on how to define ESA templates, see [Define a Template for ESA Alert Notifications](#).

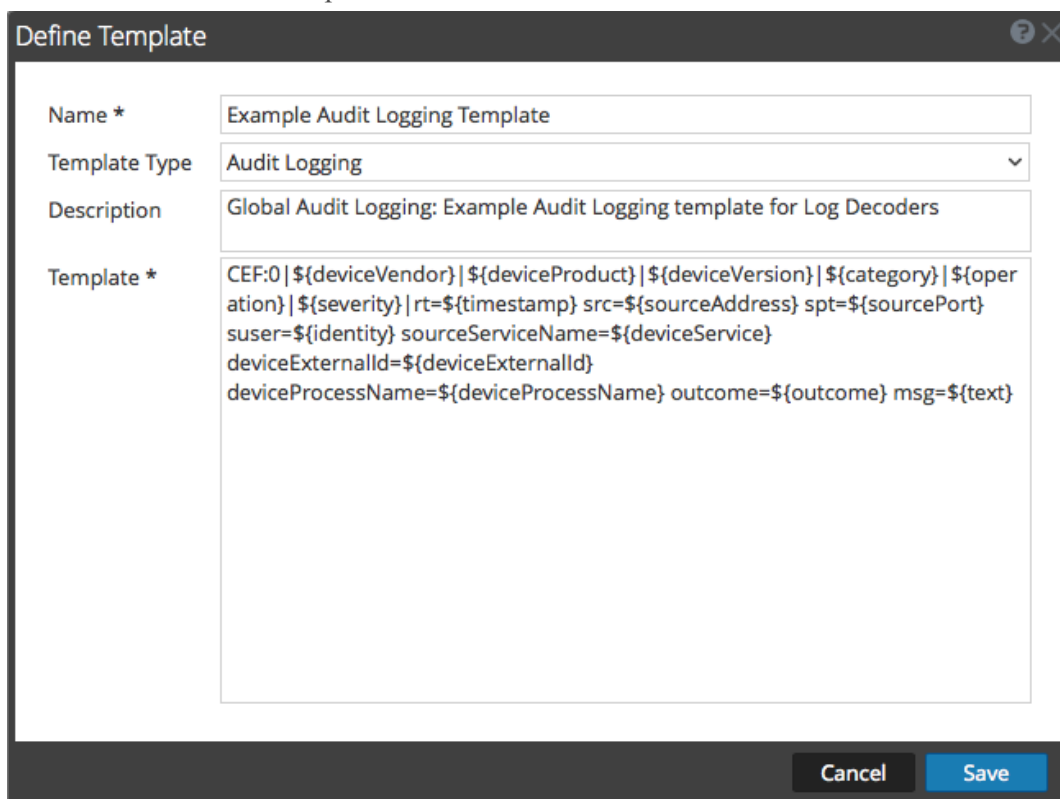
When upgrading from NetWitness Suite 10.4, all existing notification templates migrate to the Event Stream Analysis template type.

### **Add a Template**

You can use the default templates provided or you can configure your own templates. To configure your own template:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Templates** tab.
4. Click **+** to configure a template.
5. In the **Define Template** dialog, provide the following information:
  - a. In the **Name** field, type the name for the template.
  - b. In the **Template Type** field, select the type of template you want to create. For example, if you are creating a template for global audit logging, select the Audit Logging template type.
  - c. In the **Description** field, type a brief description for the template.
  - d. In the **Template** field, specify the format for the template.

- e. Click **Save** to save the template.




The **Define Template** dialog box is shown with the following fields:

- Name \***: Example Audit Logging Template
- Template Type**: Audit Logging (dropdown menu)
- Description**: Global Audit Logging: Example Audit Logging template for Log Decoders
- Template \***: CEF:0|\${deviceVendor}|\${deviceProduct}|\${deviceVersion}|\${category}|\${operation}|\${severity}|rt=\${timestamp} src=\${sourceAddress} spt=\${sourcePort} suser=\${identity} sourceServiceName=\${deviceService} deviceExternalId=\${deviceExternalId} deviceProcessName=\${deviceProcessName} outcome=\${outcome} msg=\${text}

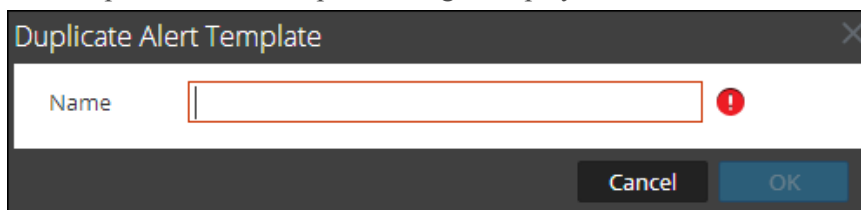
Buttons: **Cancel** and **Save**

### Duplicate a Template

You can make a copy of an existing default or user-defined template. To duplicate a template:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Templates** tab.
4. Select the template that you want to duplicate and click .

The Duplicate Alert Template dialog is displayed.



The **Duplicate Alert Template** dialog box is shown with the following fields:


- Name**: (empty text input field with a red warning icon to its right)

Buttons: **Cancel** and **OK**

5. Type the name for the duplicate template.
6. Click **OK**.


You can modify a default or user-defined template. When you edit a template, the changes are reflected only when the alert is triggered.

### Edit a Template

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Templates** tab.
4. Select a template and click .
5. In the **Define Template** dialog, modify the **Name**, **Template Type**, **Description**, and **Template** fields as required.
6. Click **Save** to save the template.

### Delete a Template

You can delete a user-defined template. When you delete a template that is used in an ESA rule, the Event Stream Analysis default template is used for alerts. You cannot delete templates associated with global audit logging configurations.

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Templates** tab.
4. Select one or more templates and click .  
A confirmation dialog is displayed.
5. Click **Yes**.  
The selected template is deleted.

## Define a Template for ESA Alert Notifications

This topic describes how you can define a template for alert notifications. Event Stream Analysis (ESA) allows you to define useful templates for alerts. You need to have a good understanding of FreeMarker and the ESA data model to define a template. For more information on FreeMarker, see [FreeMarker Template Author's Guide](#).

### ESA Data Model

Consider an ESA alert rule as shown below:



```
@Name('module_144d43f5_f0b4_4cd0_8c6c_5ce65c37e624_Alert')
@Description('Brute Force Login To Same Destination')
@RSAAalert(oneInSeconds=0, identifiers={"ip_dst"})
SELECT* FROMEvent (ec_activity = 'Logon',ec_theme = 'Authentication',ec
outcome = 'Failure',ip_dst IS NOT NULL)
.std:groupwin(ip_dst)
.win:time_length_batch(60 seconds, 2)
GROUPBYip_dst HAVING COUNT(*) = 2;
```

When a rule like the above is fired, the alert generated will have two constituent events each resembling a NextGen session with multiple meta values. The alert data-object passed to the FreeMarker template evaluator will be as follows:

```
(root)
|
| +- id = "4e67012f-9c53-4f0b-ac44-753e2c982b79" // Unique identifier for each alert
|
| +- severity = 1 // The severity of the alert
| +- time = 2013-12-31T11:02Z // The alert time (needs a ?datetime for proper rendering)
| +- moduleType = "ootb" // The module type
|
| +- moduleName = "Brute Force Login To Same Destination" // A description of the module
|
| +- statement = "module_144d43f5_f0b4_4cd0_8c6c_5ce65c37e624_Alert" // The name of the EPL statement
| +- events // The constituent events - as a sequence of event maps
| | +- [0] // offset 0 (i.e. the first constituent event)
| | | |
| | | +- event_cat_name = "User.Activity.Failed Logins"
| | | +- device_class = "Firewall" // event meta (accessible as ${events[0].device_class}$)
| | | | +- event_source_id = "uttam:50002:1703395" // Investigation URI to the individual session (used by SA)
| | | |
| | | +- ... // Other meta
| | |
| | | +- sessionid = 1703395 // NextGen sessionid
| | |
| | | +- time = 1388487764 // event/session time at NextGen source (as a long Unix timestamp)
| | |
| | | +- user_dst = "user5"
| | |
| | +- [1] // offset 1 (i.e. the second constituent event)
| | |
| | | +- device_class = "Firewall"
| | |
| | | +- event_cat_name = "User.Activity.Failed Logins"
| | |
| | | +- event_source_id = "uttam:50002:1703405"
| | |
| | | +- ...
| | |
| | | +- sessionid = 1703405
| | |
| | | +- time = 1388487766
| | |
| | | +- user_dst = "user5"
```

There are two types of template variables available in the data model:

- **Alert Meta Data:** These hold alert level details like statement name, module name, alert id, alert time, severity, and others. In FreeMarker terminology, these are top level variables associated with the alert instance itself and can be referenced simply by their names like `${moduleName}`. The `time` meta is special because it is of type `Date` and it needs to be suffixed with a `?datetime` to be properly rendered.
- **Constituent Event Meta Data:** These include the session meta fields from individual events that constitute the alert. An alert can have multiple constituent events, so there can be more than one such maps in the same alert. These show up as a sequence of hashes to the FreeMarker template evaluator and must be referenced. For instance, the alert has two constituent events the `event_source_id` for the first is available as `${events[0].event_source_id}` and the same for the second is accessible as `${events[1].event_source_id}`. You also need to be aware of which meta fields are multi-valued because those need be treated as sequences, for example `${events[0].alias_host}` will not work because it is a sequence.

**Note:** The metadata available in the constituent events for a given alert is determined by the EPL `SELECT` clause. For example, alerts from `SELECT sessionid, time FROM ...` will have only two meta values available (`sessionid`, `time`). Constituent events in `SELECT * FROM Event ...` will carry all meta fields from the `Event` type with **non-null** values.

If your template uses meta keys that are not present in all alert output, you should consider using the FreeMarker provisions for default values.

For example, if a template with text `Id=${id},ec_outcome=${ec_outcome}` is evaluated for an alert which does not include the meta key `ec_outcome` then the template evaluation fails. In such cases, you can use the missing value placeholder `${ec_outcome!"default"}`.



## Import and Export a Global Notifications Template

This topic provides instructions on how to import and export a template for notifications.

- You can export default or user-defined templates.
- You can import a template that has been exported from the NetWitness Suite instance. If you import a template with the same name as an existing template, then the existing template will be overwritten.

### Import a Template



1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.

3. Click the **Templates** tab.
4. In the toolbar, select   > **Import**.  
The **Import** dialog is displayed.
5. In the **Enter File Name** field, type the filename or click **Browse** and select the file to be imported.
6. Click **Import**.

### Export a Template

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Templates** tab.
4. Select the template you want to export.

**Note:** You can export all the templates using the   > **Export All** option.

5. In the **Actions** column, select   > **Export**.  
The **Export** dialog is displayed.
6. In the **Enter File Name** field, type the filename.
7. Click **Save**.

## Configure Email Servers and Notification Accounts

This topic provides instructions for configuring email so that users can receive notifications in NetWitness Suite. RSA NetWitness® Suite can send notifications to users via email about various system events. To be able to configure these email notifications, you must first configure the SMTP email server. The Email Configuration panel provides a way to:

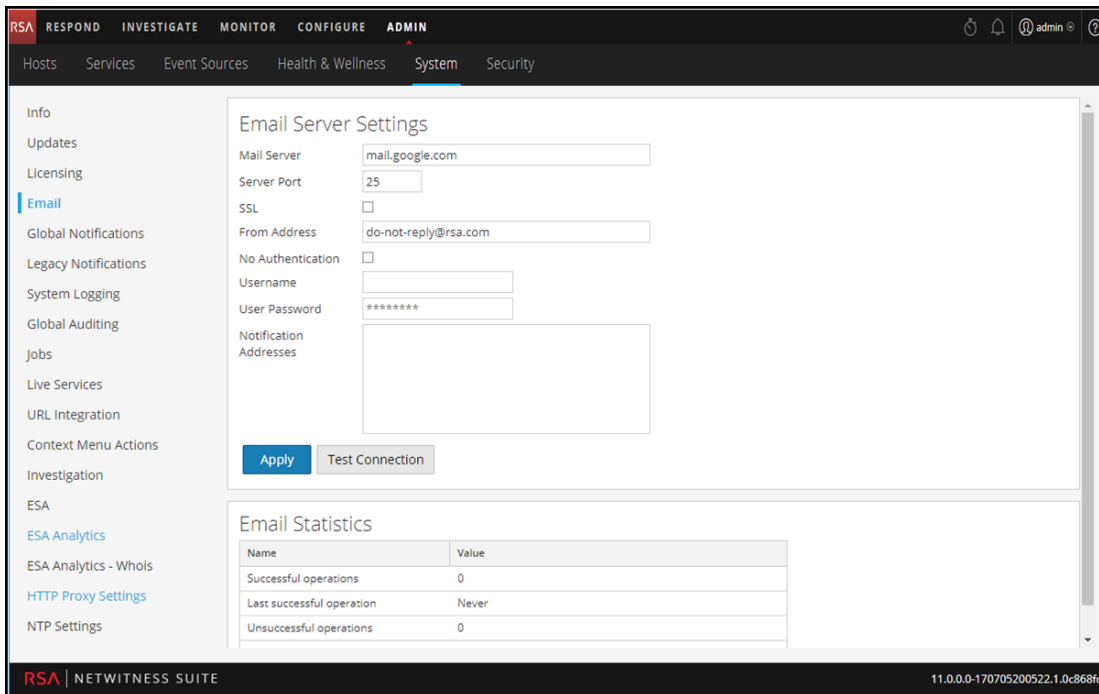
- Configure the email server.
- Set up an email account to receive notifications.
- View statistics on email operations.

NetWitness Suite requires access to an SMTP mail server in order to send reports to users. Each user account can be configured to receive emailed reports. These reports can be generated manually, through the user interface, or automatically, through the auditing system. The following guidelines apply:

- Any SMTP mail host can be used to deliver emails, and each host requires a different configuration. The SMTP provider provides the settings for configuration.
- Some SMTP servers require user authentication in order to relay emails successfully. Typically, this is the login and password for the email account.
- Best practice is to create a new, dedicated email account on the SMTP email server for NetWitness Suite reports.

To configure NetWitness Suite email notifications:

1. Go to **ADMIN > System**.  
The Administration System view is displayed.
2. In options panel, select **Email**.



The screenshot displays the NetWitness Suite Administration System interface. The top navigation bar includes 'ADMIN' and 'System'. The left sidebar shows the 'Email' option selected. The main content area is titled 'Email Server Settings' and contains the following fields:

- Mail Server: mail.google.com
- Server Port: 25
- SSL:
- From Address: do-not-reply@rsa.com
- No Authentication:
- Username: [empty field]
- User Password: [masked field]
- Notification Addresses: [empty text area]

Buttons for 'Apply' and 'Test Connection' are located below the settings. Below the settings is an 'Email Statistics' table:

Name	Value
Successful operations	0
Last successful operation	Never
Unsuccessful operations	0

The bottom of the interface shows the RSA | NETWITNESS SUITE logo and the version number 11.0.0.0-170705200522.1.0-868fd.

3. If you want to change the default mail server, specify the **Mail server** name and **Server port**.
4. If the email server communicates with NetWitness Suite using SSL, check the box next to **Use SSL**.
5. In the **From address** field, type the name of the email account sending NetWitness Suite email notifications.
6. If the SMTP server requires user authentication to relay emails successfully, type the **Username** and **User Password** for logging in to the email account.

7. To activate the settings, click **Apply**.

You can now configure NetWitness Suite modules to receive various notifications by email.

## Configure Global Audit Logging

Global Audit Logging provides NetWitness Suite Auditors with consolidated visibility into user activities within NetWitness Suite in real-time from one centralized location. This visibility includes audit logs gathered from the NetWitness Suite system and the different services throughout the NetWitness Suite infrastructure.

NetWitness Suite audit logs collect in a centralized system that converts them into the required format and forwards them to an external syslog system. The external syslog system can be a third-party syslog server or a Log Decoder.

You configure global audit logging in the Global Audit Logging Configurations panel. An audit logging template defines the format and message fields of the audit log entries. A Syslog Notification Server configuration defines the destination to send the audit logs. If you want to forward audit logs to a Log Decoder, configure a Syslog type of Notification Server for the Log Decoder.

The following are some of the user actions logged from NetWitness Suite:

- User login success
- User login failure
- User logouts
- Maximum Login failures exceeded
- All UI pages accessed
- Committed configuration changes (including when a user changes their own password)
- Queries performed by the user
- User access denied
- Data export operations

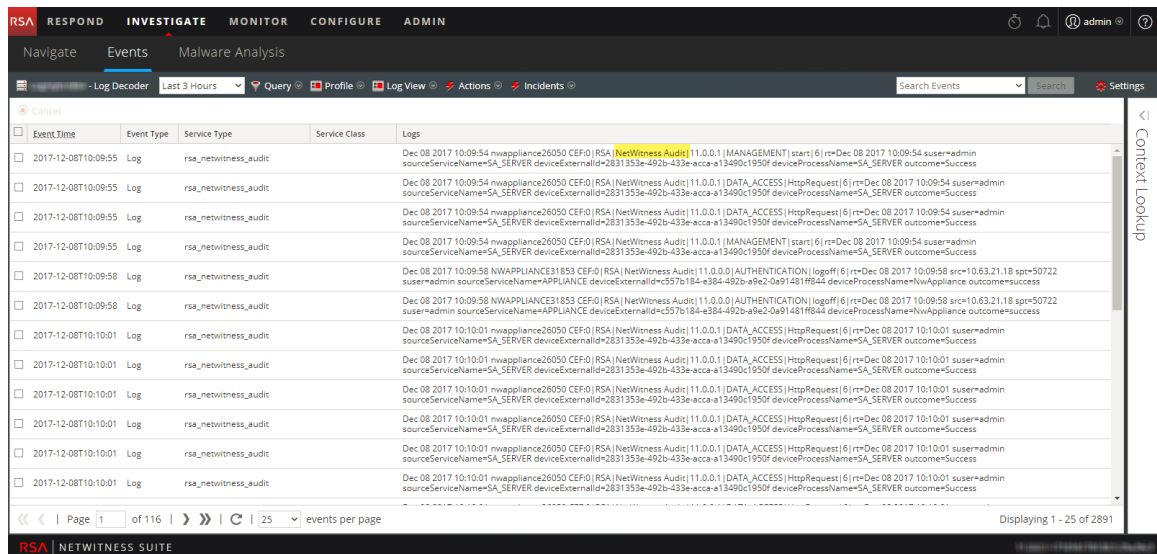
After you create a global audit logging configuration, audit logs containing these user actions automatically go to the external syslog system in the format specified in the selected Audit Logging template. You can create multiple global audit logging configurations for different destinations that use different templates. For example, you can create a global audit logging configuration for an external Syslog server with a template that contains all of the available meta keys and another configuration for a Log Decoder with a template that contains selected meta keys.

For Log Decoders, you use the Default Audit CEF Template. You can add or remove fields from the Common Event Format (CEF) template if you have specific requirements. [Define a Template for Global Audit Logging](#) provides instructions and [Supported CEF Meta Keys](#) describes the CEF meta keys available to use in the audit logging templates.

For third-party syslog servers, you can use a default audit logging template or define your own format (CEF or non-CEF). [Define a Template for Global Audit Logging](#) provides instructions and [Supported Global Audit Logging Meta Key Variables](#) describes the available variables.

Auditors can view the audit logs on the selected Log Decoder or third-party syslog server. If using a Log Decoder, auditors can view the audit logs using NetWitness Suite Investigations or Reports.

The following figure shows global audit logs in Investigation (INVESTIGATE > Events).



For examples of some of the user actions logged, see [Add New Configuration Dialog](#). For a list of message types being logged by the various NetWitness Suite components, see [Global Audit Logging Operation Reference](#).

## Global Audit Logging - High-Level Procedure

Global Audit Logging is configured in the Global Audit Logging Configurations panel, which is accessed from ADMIN > System view > Global Auditing. Before you can configure Global Audit Logging, you need to configure a Syslog Notification Server and an Audit Logging template. A Syslog Notification Server defines the destination to send the audit logs. An Audit Logging template defines the format and message fields of the audit log entry.

The Global Audit Logging Configuration panel provides a **view settings** link that takes you to the Global Notifications panel (Administration System view > Global Notifications) where you can configure the Syslog Notification Server and Audit Logging template.

Perform the following procedures in the order shown to configure Global Audit Logging.

Procedures	Reference / Instructions
1. Configure a Syslog Notification Server.	<p>Configure a Syslog Notification Server to use for Global Audit Logging. You can define a third-party syslog server or Log Decoder as a destination to receive the audit logs.</p> <p><a href="#">Configure a Destination to Receive Global Audit Logs</a>. Global Audit Logging configurations use the Syslog notification server type. If you want to forward audit logs to a Log Decoder, create a Notification Server of the Syslog type.</p>
2. Select or configure an Audit Logging template to use.	<p>Select an Audit Logging template for the Syslog notification server. You can use a default Audit Logging template or define your own audit logging template. Global Audit Logging configurations use the Audit Logging template type and a Syslog notification server.</p> <p><a href="#">Configure Templates for Notifications</a> provides additional information.</p> <p>For Log Decoders, use the <b>Default Audit CEF Template</b>. You can add or remove fields from the Common Event Format (CEF) template if you have specific requirements. Define a Template for Global Audit Logging provides instructions.</p> <p>For third-party syslog servers, you can use a default audit logging template or define your own format (CEF or non-CEF). <a href="#">Define a Template for Global Audit Logging</a> provides instructions and Supported Global Audit Logging Meta Key Variables describes the available variables.</p>
3. (Optional - Only if consuming with a Log Decoder) Deploy the Common Event Format parser to your Log Decoder from Live.	<p>Ensure that you have deployed and enabled the latest Common Event Format parser from Live. Find and Deploy Live Resources and Enable and Disable Log Parsers provide instructions.</p>



Procedures	Reference / Instructions
4. Define a global audit logging configuration, which defines how the global audit logs are forwarded to external Syslog systems.	<a href="#">Define a Global Audit Logging Configuration</a> provides instructions. After you add a Global Audit Logging configuration, audit logs are forwarded to the selected Notification Server in the configuration.
5. Verify that the global audit logs show the audit events.	Test your audit logs to ensure that they show the audit events as defined in your audit logging template. <a href="#">Verify Global Audit Logs</a> provides instructions.



## Configure a Destination to Receive Global Audit Logs

In Global Audit Logging, Syslog Notification Servers are the configurations that define the destinations to receive global audit logs. You need to configure a Syslog Notification Server to use Global Audit Logging. You can define a third-party syslog server or a Log Decoder as the destination to receive the audit logs.

### Configure a Syslog Notification Server for a Third-Party Syslog Server

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Servers** tab.

**Note:** You do not need to configure the Output tab for Global Audit Logging.

4. From the   drop-down menu, select **Syslog**.  
The **Define Syslog Notification Server** dialog is displayed.

**Define Syslog Notification Server**

Provides auditing through the use of the RFC 5424 syslog protocol. Regulations, such as SOX, PCI DSS, HIPAA, and many others are requiring organizations to implement comprehensive security measures, which often include collecting and analyzing logs from many different sources. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis.

Enable

Name\*

Description

Server IP Or Hostname\*

Server Port

Protocol

Facility

Max Alerts Per Minute

Max Alert Wait Queue Size:  ?

**Cancel** **Save**

5. Configure the Syslog notification server as described in the following table.

Field	Description
Enable	Select to enable the notification server.
Name	A name to identify or label the third-party syslog server.
Description	(Optional) A brief description of the notification server.
Server IP or Hostname	The third-party syslog server hostname or IP address.
Server Port	The port number where the target syslog process is listening.
Protocol	The protocol to be used for transferring formatted audit logs to the third-party syslog server.
Facility	The syslog facility to be used for writing formatted audit logs to the third-party syslog server.



The **Max Alerts Per Minute** and **Max Alert Wait Queue Size** fields are not used for Global Audit Logging.

6. Click **Save**.

#### **Configure a Syslog Notification Server for a Log Decoder**

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. Click the **Servers** tab.

**Note:** You do not need to configure the Output tab for Global Audit Logging.

4. From the   drop-down menu, select **Syslog**.  
The **Define Syslog Notification Server** dialog is displayed.

### Define Syslog Notification Server ? X

Provides auditing through the use of the RFC 5424 syslog protocol. Regulations, such as SOX, PCI DSS, HIPAA, and many others are requiring organizations to implement comprehensive security measures, which often include collecting and analyzing logs from many different sources. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis.

Enable

Name\*

Description

Server IP Or Hostname\*

Server Port

Protocol

Facility

Max Alerts Per Minute

Max Alert Wait Queue Size:  ?

5. Configure the Syslog notification server as described in the following table.

Field	Description
Enable	Select to enable the notification server.
Name	A name to identify or label the Log Decoder syslog notification server.
Description	(Optional) A brief description of the notification server.
Server IP or Hostname	The Log Decoder hostname or IP address.
Server Port	The port number where the target syslog process is listening.
Protocol	The protocol to be used for transferring formatted audit logs to the Log Decoder.
Facility	The Syslog facility to be used for writing formatted audit logs to the Log Decoder.

The **Max Alerts Per Minute** and **Max Alert Wait Queue Size** fields are not used for Global Audit Logging.

6. Click **Save**.

## Next Steps

Select a default Audit Logging template to use for Global Audit Logging. If necessary, you can define your own custom template. [Define a Template for Global Audit Logging](#) provides additional information.

### Define a Template for Global Audit Logging

This topic provides instructions on how to define an audit logging template to use for Global Audit Logging. Before you configure Global Audit Logging, configure a Syslog notification server and select an Audit Logging template. You can choose to use a default audit logging template or you can define your own template.

NetWitness Suite includes two default audit logging templates:

- **Default Audit CEF Template:** You can use this template for Log Decoders and third-party syslog servers.
- **Default Audit Human-Readable Format:** You can use this template only for third-party syslog servers. Do not forward messages from this template to a Log Decoder.

The first procedure provides instructions on how to define an audit logging template for a Log Decoder. The audit logging template defines the format and message fields of the audit logs sent to the Log Decoder or third-party syslog server.

Global audit logging templates that you define for a Log Decoder use Common Event Format (CEF) and must meet the following specific standard requirements:

- Include the CEF headers in the template.
- Use only the extensions (Key=Value) listed in the [Supported CEF Meta Keys](#) table.
- Ensure that the extensions are in the `key=${string}<space>key=${string}` format.

The second procedure provides instructions on how to define a custom global audit logging template in human-readable format for a third-party syslog server. For third-party syslog servers, you can define your own format (CEF or non-CEF).

### Define a Global Audit Logging Template for a Log Decoder

You can use the **Default Audit CEF Template** to send global audit logs to a Log Decoder. To define your own template:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.

3. Click the **Templates** tab.
4. Click **+** to configure a template.
5. In the **Define Template** dialog, provide the following information:
  - a. In the **Name** field, type the name for the template.
  - b. In the **Template Type** field, select the **Audit Logging** template type.
  - c. In the **Description** field, type a brief description for the template.
  - d. In the **Template** field, enter the format for the audit logging template.  
The following format is a customized template provided as an example. It differs from the default CEF template.

```
CEF:0|${deviceVendor}|${deviceProduct}|${deviceVersion}|${category}
|${operation}|${severity}| rt=${timestamp} src=${sourceAddress}
spt=${sourcePort}
suser=${identity} sourceServiceName=${deviceService}
deviceExternalId=${deviceExternalId} dst=${destinationAddress}
dpt=${destinationPort} dvcpid=${deviceProcessId}
deviceProcessName=${deviceProcessName} outcome=${outcome}
msg=${text}
```

The highlighted CEF syslog header is required to conform to the CEF standard and is a requirement for the CEF parser in the Log Decoder. The other keys are optional and you can configure them. See all the supported meta keys that are supported by the CEF parser in the Log Decoder in the [Supported CEF Meta Keys](#) table.

**Note:** Use all of the extensions in the following format:

```
deviceProcessName=${deviceProcessName} outcome=${outcome}
```

Include a <space> between each key=\${string} pair in the extension keys section.

## 6. Click Save.

After you define the CEF audit logging template, ensure that you have deployed and enabled the latest Common Event Format (CEF) parser from Live. "Find and Deploy Live Resources" and "Enable and Disable Log Parsers" in the *Live Services Management Guide* and *Decoder and Log Decoder Configuration Guide* provide instructions.

**Note:** If you need to use a specific meta key for Investigations and Reporting, ensure that the meta keys that you select are indexed in the **table-map.xml** file on the Log Decoder. If they are not indexed, follow the Maintain the Table Map Files topic in the *Host and Services Configuration Guide* procedure to update the table mappings. Ensure that the meta keys are also indexed in the **index-concentrator.xml** on the Concentrator. "Edit a Service Index File" topic in the *Host and Services Configuration Guide* provides additional information.

### Define a Custom Global Audit Logging Template

For third-party syslog servers, you can define your own template format (CEF or non-CEF). You can use the **Default Audit Human-Readable Format** template to send global audit logs to a third-party syslog server in a format that is easier to read than the CEF format. If you want to define your own template in human-readable format, follow this procedure.

For Log Decoders, you must use a CEF template with some specific requirements. The *Define an Audit Logging Template for a Log Decoder* procedure above provides instructions for creating a template in CEF format.

To define a custom global audit logging template in human-readable format:

1. Go to **ADMIN > System**.
2. In the left navigation panel, select **Notifications**.
3. Click the **Templates** tab.
4. Click **+** to configure a template.
5. In the **Define Template** dialog, provide the following information:
  - a. In the **Name** field, type the name for the template.
  - b. In the **Template Type** field, select the **Audit Logging** template type.
  - c. In the **Description** field, type a brief description for the template.
  - d. In the **Template** field, enter the format for the audit logging template. The following example is in human-readable format with selected meta key variables.

```
${timestamp} ${deviceService} [audit] Event Category: ${category}
Operation: ${operation} Outcome: ${outcome} Description: ${text}
User: ${identity} Role: ${userRole}
```

You can use any of the meta key variables that are supported by global audit logging shown in the [Supported Global Audit Logging Meta Key Variables](#) table.



## 6. Click Save.

The screenshot shows a 'Define Template' dialog box with the following fields and values:

- Name \***: Custom GAL Template
- Template Type**: Audit Logging
- Description**: Custom Human-Readable Template
- Template \***: `${timestamp} ${deviceService} [audit] Event Category: ${category} Operation: ${operation} Outcome: ${outcome} Description: ${text} User: ${identity} Role: ${userRole}`

Buttons at the bottom: Cancel, Save

The following example shows global audit logs in human-readable format for this template:

```
06 2015 14:16:04 REPORTING_ENGINE [audit] Event Category: CONFIGURATION
Operation: Set Outcome: null Description: null User: admin Role:
Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY

Apr 06 2015 14:16:04 REPORTING_ENGINE [audit] Event Category:
CONFIGURATION Operation: IPDBConfig Outcome: SUCCESS Description: Config
update event occurred User: admin Role:
Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY

Apr 06 2015 14:16:04 NW_SERVER [audit] Event Category: DATA_ACCESS
Operation: /admin/1/config Outcome: Success Description: null User:
admin Role: Administrators+Administrators+PRIVILEGED_CONNECTION_
AUTHORITY
```

### Next Step

[Define a Global Audit Logging Configuration](#) provides instructions for defining a global audit logging configuration for NetWitness Suite.

## Define a Global Audit Logging Configuration

This topic tells administrators how to define a global audit logging configuration. This procedure is required only if you choose to set up centralized audit logging in your environment. These global audit logging configurations define how the global audit logs are forwarded to external syslog systems or Log Decoders. Audit logs are forwarded to the selected Notification Servers.

### Prerequisites

Before starting this procedure, configure the following to use for global audit logging:

- Syslog Notification Server
- Audit Logging Template

You configure the notification server and template on the Global Notifications panel. You can access the Global Notifications panel by clicking the **view settings** link on the Global Audit Logging Configurations panel. You can only define a Syslog type of Notification Server for global audit logging. For Log Decoders, use a Syslog type of Notification Server and a Common Event Format (CEF) audit logging template. You can use a default audit logging template or define your own template. You can create multiple audit logging templates and Syslog Notification Servers to use for your global audit logging configurations.

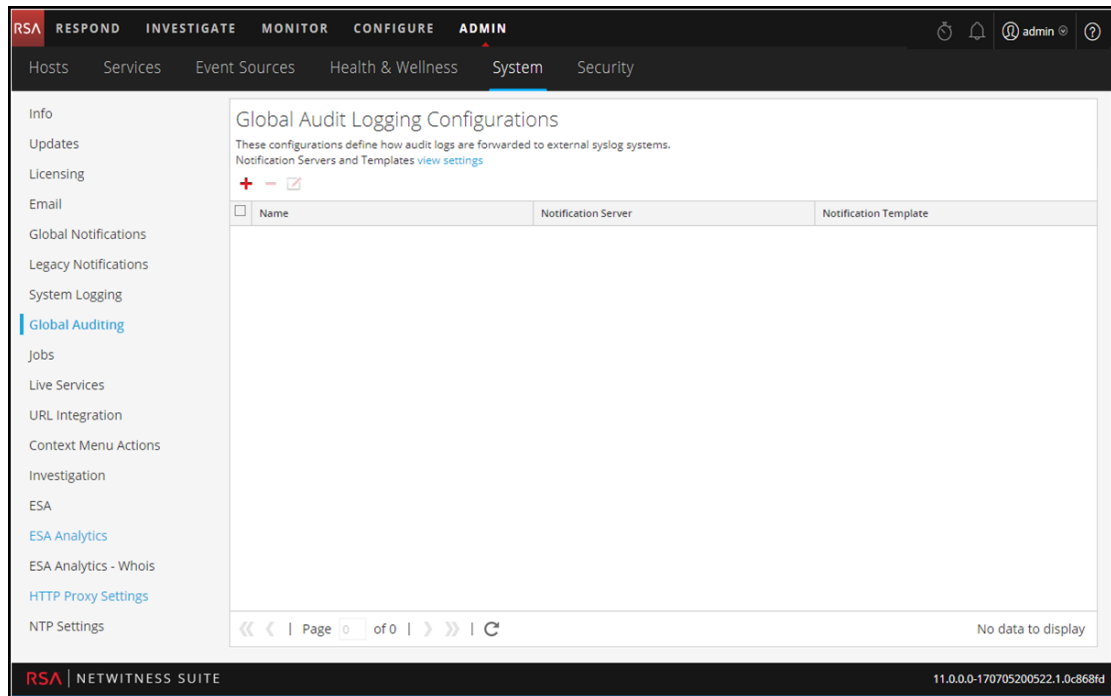
If you are forwarding global audit logs to a Log Decoder, deploy the Common Event Format parser to your Log Decoder from Live.

### Add a Global Audit Logging Configuration

1. Go to **ADMIN > System**.

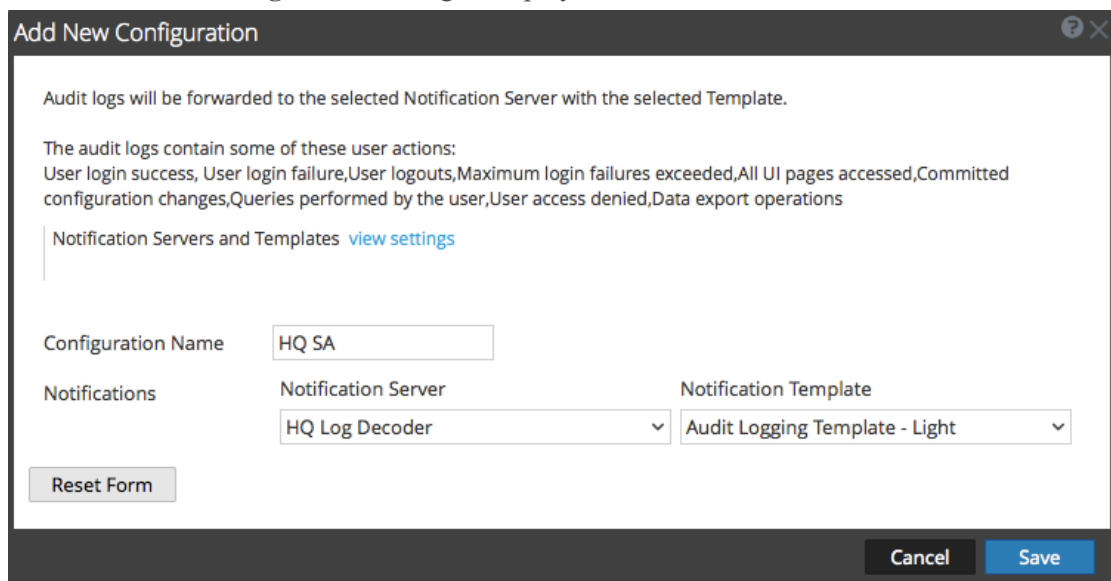
2. In the options panel, select **Global Auditing**.

The **Global Audit Logging Configurations** panel is displayed.



3. Click **+** to add a global audit logging configuration.

The **Add New Configuration** dialog is displayed.



4. In the **Configuration Name** field, type a unique name for the global audit logging configuration. For example, you can create a configuration for a specific type of global audit logging configuration, such as HQ NW for a NetWitness Suite headquarters configuration.


5. In the **Notifications** section, select the syslog **Notification Server** to use for this configuration. The notification server is the destination to send the global audit logs.
6. Select the audit logging **Notification Template** to use for this configuration. The Audit Logging template defines the format and audit log message fields to be sent.
7. Click **Save**.

Add New Configuration Dialog provides additional information and examples of the user actions logged. For a list of message types being logged by the various NetWitness Suite components, see [Global Audit Logging Configurations Panel](#).

### **Edit a Global Audit Logging Configuration**

This topic provides instructions on how to edit a global audit logging configuration. You can edit a global audit logging configuration to change the destination of the global audit logs for your user audits by selecting a different Notification Server. You can also change the format and message fields of the global audit log entries by selecting a different Notification Template. You make changes to the Notification Server or Template on the Global Notifications panel. You can access the Global Notifications panel by clicking the **view settings** link on the Global Audit Logging Configurations panel.

You cannot change which NetWitness Suite user actions are logged and sent in the global audit logs.

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Auditing**.
3. In the **Global Audit Logging Configurations** panel, select a configuration to edit and click .
4. In the **Add New Configuration** dialog, modify the global audit logging configuration as required. You can modify the **Configuration Name** and select a different **NotificationServer** or **Template**.
5. Click **Save**.

### **Delete a Global Audit Logging Configuration**

Deleting a global audit configuration does not delete the associated notification server and template. After you delete a global audit logging configuration, the forwarding of global audit logs specified in that configuration is discontinued.

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Auditing**.

3. In the **Global Audit Logging Configurations** panel, select a configuration to delete and click .

A confirmation dialog is displayed.

4. Click **Yes**.

The selected configuration is deleted.

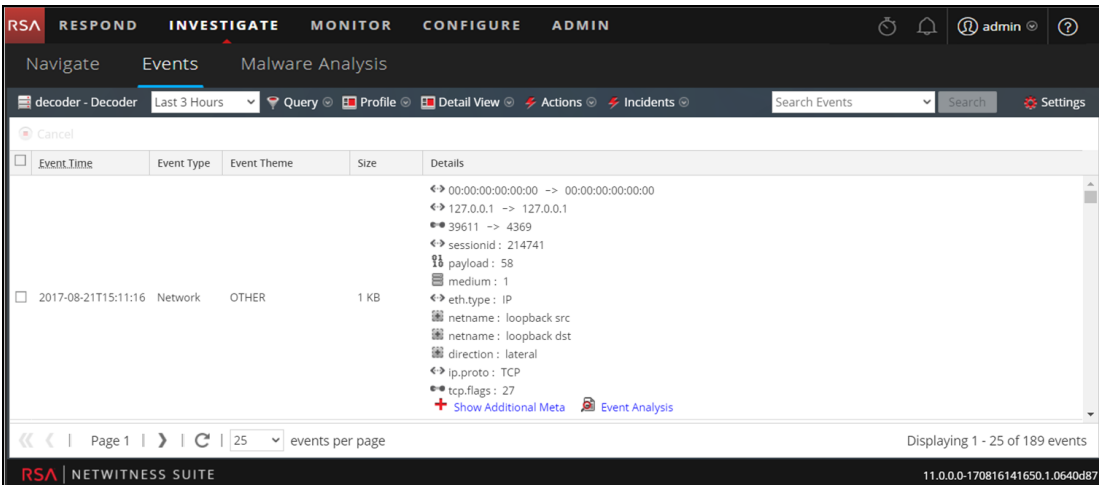
## Verify Global Audit Logs

This topic provides instructions on how to verify global audit logs. After you have configured global audit logging, you need to test your global audit logs to ensure that they show the audit events as defined in your global audit logging template.

Before starting this task, complete the steps detailed in [Configure Global Audit Logging](#).

To view and verify the global audit logs if you are using a Log Decoder:

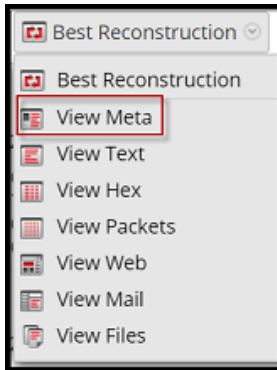
1. Go to **Investigate > Events**.
2. From within the Navigate view, select the Log Decoder, and click **Navigate**.



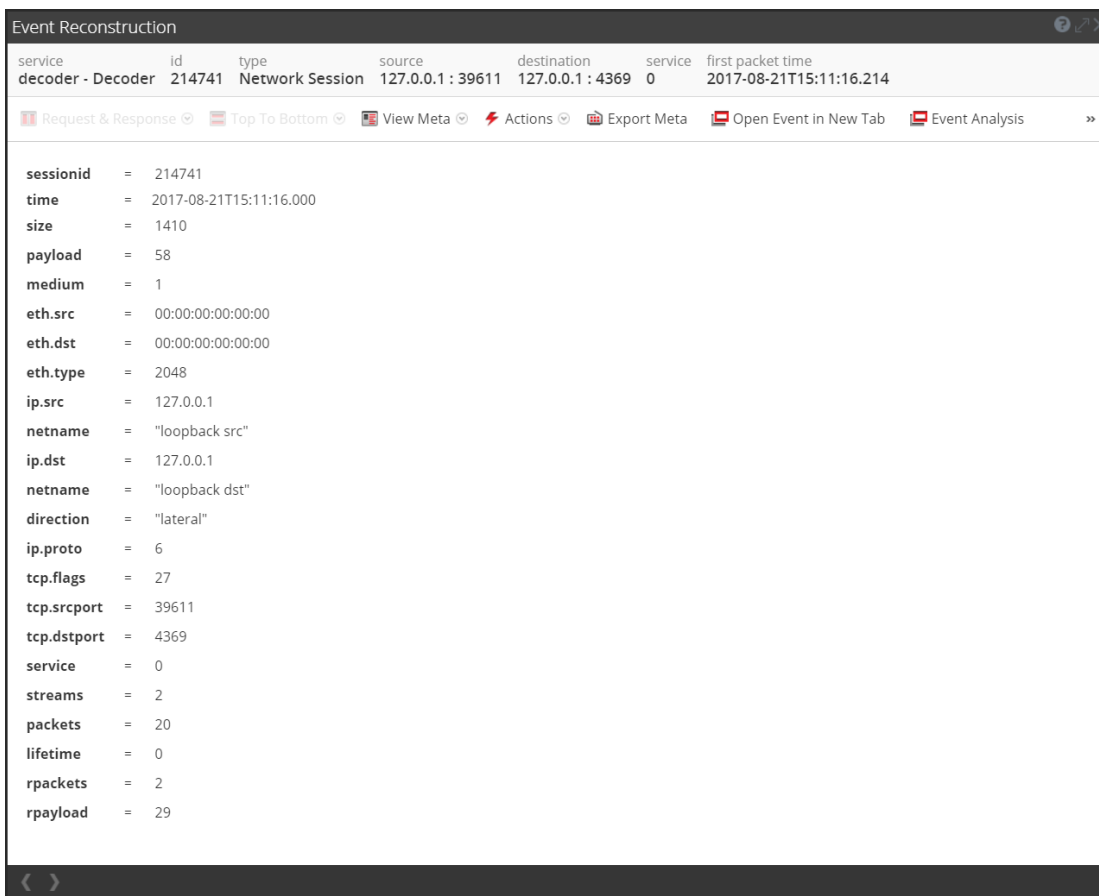
Event Time	Event Type	Event Theme	Size	Details
2017-08-21T15:11:16	Network	OTHER	1 KB	<ul style="list-style-type: none"> <li>00:00:00:00:00:00 -&gt; 00:00:00:00:00:00</li> <li>127.0.0.1 -&gt; 127.0.0.1</li> <li>39611 -&gt; 4369</li> <li>sessionid : 214741</li> <li>payload : 58</li> <li>medium : 1</li> <li>eth.type : IP</li> <li>netname : loopback src</li> <li>netname : loopback dst</li> <li>direction : lateral</li> <li>ip.proto : TCP</li> <li>tcp.flags : 27</li> </ul>

3. Compare the fields in the global audit logs with the fields defined in the global audit logging template that you used in your global audit logging configuration.

4. Double-click a log and in the Event Reconstruction dialog, select **View Meta**.



5. Verify that the meta that you want to audit is correct.



## Example CEF Output

The following example shows global audit logs for an audit logging Common Event Format (CEF) template.

**Template:**

```
CEF:0|${deviceVendor}|${deviceProduct}|${deviceVersion}|${category}|${o
per
ation}|${severity}| rt=${timestamp} src=${sourceAddress}
spt=${sourcePort}
suser=${identity} sourceServiceName=${deviceService}
deviceExternalId=${deviceExternalId} dst=${destinationAddress}
dpt=${destinationPort} dvcpid=${deviceProcessId}
deviceProcessName=${deviceProcessName} outcome=${outcome} msg=${text}
```

**Example logs:**

```
2017-04-09T18:45:46.313096+00:00 <hostname> CEF:0|RSA|Security Analytics
Audit|11.0.0.0|AUTHENTICATION|login|6|rt=Apr 09 2017 18:45:46
src=10.20.252.197 spt=51366 suser=admin sourceServiceName=LOG_DECODER
deviceExternalId=96b08193-a9d0-4a79-b362-87b56851f411 outcome=success

2017-04-09T18:45:46.322132+00:00 <hostname> CEF:0|RSA|Security Analytics
Audit|11.0.0.0|AUTHENTICATION|logoff|6|rt=Apr 09 2017 18:45:46
src=10.20.204.33 spt=47690 suser=admin sourceServiceName=BROKER
deviceExternalId= 314fb8c8-afe4-4249-9468-a36035008a52 outcome=success

2017-04-09T18:45:46.325792+00:00 <hostname> CEF:0|RSA|Security Analytics
Audit|11.0.0.0|AUTHENTICATION|logoff|6|rt=Apr 09 2017 18:45:46
src=10.20.252.197 spt=59495 suser=admin sourceServiceName=CONCENTRATOR
deviceExternalId= 96b08193-a9d0-4a79-b362-87b56851f411 outcome=success
```

Where <hostname> is the syslog header hostname (alias.host).

For CEF templates, if an audit event does not have a value for a field in the template, then the corresponding event arriving at the third party syslog server or Log Decoder will have the field removed.

## Example Human-Readable Format Output

The following example shows global audit logs for an audit logging human-readable format template on a third-party syslog server.

**Template:**

```
${timestamp} ${deviceService} [audit] Event Category: ${category}
Operation: ${operation} Outcome: ${outcome} Description: ${text}
User: ${identity} Role: ${userRole}
```

**Example logs:**

```
06 2017 14:16:04 REPORTING_ENGINE [audit] Event Category: CONFIGURATION
Operation: Set Outcome: null Description: null User: admin Role:
Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY

Apr 06 2017 14:16:04 REPORTING_ENGINE [audit] Event Category:
CONFIGURATION Operation: IPDBConfig Outcome: SUCCESS Description: Config
update event occurred User: admin Role:
Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY

Apr 06 2017 14:16:04 SA_SERVER [audit] Event Category: DATA_ACCESS
Operation: /admin/1/config Outcome: Success Description: null User:
admin Role: Administrators+Administrators+PRIVILEGED_CONNECTION_
AUTHORITY
```

## Configure Investigation Settings

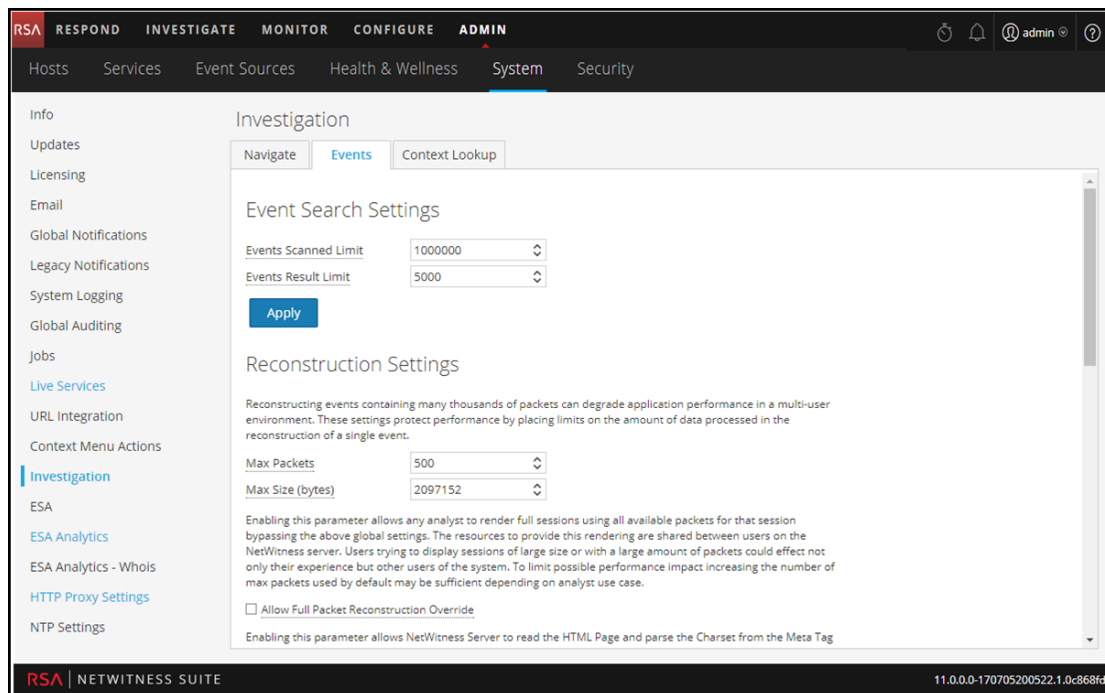
This topic provides instructions for administrators who are configuring the settings that apply to all Investigations on the NetWitness Suite instance being configured. The settings for configuring and tuning behavior of NetWitness Suite Investigation are available in the System view > Investigation panel. These settings apply to all investigations and reconstructions on the current instance of NetWitness Suite.

### Configure Navigate, Events, and Context Lookup Settings

1. Go to **ADMIN > System**.



- In the options panel, select **Investigation**.  
The Investigation Configuration panel is displayed.



- In the **Navigate** tab, in the **Render Threads Settings** field, select the maximum number of concurrent meta key values that are loaded by a single user in the navigate view. Click **Apply**.
- In the **Navigate** tab, in the **Parallel Coordinates Settings** section, set the maximum limits for meta values scanned and meta value results that can be included in a parallel coordinates visualization. For better performance, these are the recommended settings: Meta Values Scan Limit -100000 and Meta Values Result Limit to 1,000-10,000  
Click **Apply**.
- In the **Events** tab, in the **Event Search Settings** section, set the maximum numbers of events scanned and event results displayed when an analyst is conducting an event search in the Events view. Click **Apply**.
- In the **Events** tab, in the **Reconstruction Settings** section, set the limits for the amount of data processed in the reconstruction of a single event. The default values are 100 maximum packets and 2097152 bytes. If analysts are seeing slow performance when reconstructing sessions in Investigation, the reconstructing settings may need adjustment. Click **Apply**.

**Caution:** Setting a higher value affects the performance of the NetWitness Server by increasing the time and memory taken to create a reconstruction of an event. Setting the value to zero disables any limit and may lead to a NetWitness Server crash.

7. (Optional) In the **Events** tab, in the **Web View Reconstruction Settings** section, enable the use of supporting files in a web view reconstruction, and configure the additional settings to calibrate web view reconstructions. These include the time range (in seconds) to scan for related events, the maximum number of related events to scan, and overrides to Reconstruction Settings for use with web view reconstructions. Click **Apply**.
8. In the **Context Lookup** tab, manage mapping of Context Hub meta types with meta keys in Investigation. You can add or remove meta keys to the list of meta types supported in Investigation by Context Hub. Procedures associated with this are provided in "Manage Meta Type and Meta Key Mapping" in the *Context Hub Configuration Guide*.

**Note:** The options on the Context Lookup tab are only available if the Context Hub service is configured.

## Clear Reconstruction Cache for Services

Under Reconstruction Cache Settings, administrators can clear the cache for one or more services. For example, the administrator can clear the cache for a single Broker, a Broker and Decoder, or all connected services. These are a few examples of causes for stale cache being used in a reconstruction.

- The downstream services may have their sessions invalidated or data reset. As an example, if Investigation is browsing a Broker and a downstream Concentrator or Decoder has a data reset, the meta and session data for the investigating service (Broker) does not match the content if the downstream service has reset and repopulated. The reconstruction in Investigation shows content from cache, which does not match the real content. Even if the Decoder is offline, content is still displayed in the Broker reconstruction. Clearing cache on the Broker causes the NetWitness Suite to reach out to the Decoder and an error is returned because the Decoder is offline.
- Another case where cache may be stale is when a service ID for a downstream service changes. This can happen when exporting, importing, deleting, and adding services to NetWitness Suite because NetWitness Suite can reuse service IDs. In this case, clearing the cache on the Broker causes NetWitness Suite to request data from the services.

To clear reconstruction cache, do one of the following:

1. To clear cache for one or more services, select the services and click **Clear Cache for the Selected Services**.

2. To clear the cache for all listed services, click **Clear Cache for All Services**.  
The reconstruction cache for the selected services is cleared. NetWitness Suite sends a request for data to the services.

## Configure Live Services Settings

Options for configuring Live Services are in the System view > Live Services Configuration panel. The Live Configuration panel allows you to configure:

- The Live account.
- The Live Content update schedule and preferences for notification of updates.
- Participation in Live Services Feedback.
- Sharing Live Content Usage
- RSA Live Connect (Beta)

## Prerequisite

To activate your Live account for NetWitness Suite, please contact RSA Customer Care. When you have a confirmation that your Live account has been set up, you can configure and test the CMS server connection.

When you log on to NetWitness Suite for the first time, you are prompted with **New Features Enabled** dialog.

New Features Enabled

RSA has introduced several new Live Services that will enhance the experience of detecting threats. Below is a list of all the new services that will be enabled :

- ✔ **Live Feedback**  
 Customer usage data, including usage metrics, threat detection enabled, number of enabled ESA rules and current version of SA hosts, shall automatically be shared with RSA upon this system's connection to the Internet. This data is automatically shared only if Live account is configured and shall be protected in accordance with the applicable license agreement. All such data shall be anonymized and shall not have any Personally Identifiable Information. [Learn about the data RSA is collecting.](#)  
[Show less](#)
- ✔ **RSA Live Connect (Beta)**  
 RSA Live Connect is a cloud based threat intelligence service.This service collects, analyzes, and assesses threat intelligence data such as IP addresses, domains, and files collected from various sources including the RSA Security Analytics and RSA ECAT customer community.The threat intelligence data is de-identified, encrypted, and sent securely and anonymously over SSL to the RSA Live Connect cloud service and stored in a secure environment.This threat intelligence information can be leveraged by analysts for identifying and investigation potential security threats.  
[Show less](#)
- ✔ **Threat Insights**  
 This Live Connect option provides analysts the opportunity to pull threat intelligence data such as IP related information from the Live Connect service to be leveraged by analysts during investigation. In addition, analysts can voluntarily provide anonymous risk assessment feedback on the specific intelligence to Live Connect.  
[Show less](#)
- ✔ **Analyst Behaviors**  
 This Live Connect option is an automated data collection service. It is responsible for gathering meta data captured locally by Security Analytics and securely sending it to RSA Live Connect.This data will be leveraged for deep analysis to drive and improve the RSA Live and Live Connect threat intelligence services in order to proactively identify potential security threats.  
[Show less](#)

*NOTE: The type of data that potentially could be shared from a user's network to the RSA Live Connect cloud service could encompass various types of meta data captured by the Security Analytics product such as ip.src, ip.dst, ip.addr, device.ip, alias.ip, alias.host, paddr, sessionid, domain.dst, domain.src.*

Customers who do not wish to receive threat intelligence and/or share de-identified and anonymized information with the Live Connect service should change their settings in the [Live Connect](#) feature and/or contact RSA Customer Support for more information.

To take advantage of these services Live connection is required. If Live is already connected, these services will be enabled automatically. You can change the setting by clicking the "View Settings" button.

View Settings
Accept

When you click **Accept**, you automatically agree to the following:

- Participate in Live Feedback.
- Use Live Connect features to receive threat intelligence data.
- Allow NetWitness Suite to send anonymous, technical data about your environment to RSA.

If you click **View Settings**, you are redirected to the Live Services user interface to view the settings for Live Feedback and Live Connect Threat Data Sharing. If you have not configured the Live Account a masked screen is displayed.

For information on Analyst Behaviors and Data Sharing, see the "NetWitness Suite Feedback and Data Sharing" topic in the *Live Services Management Guide*.

## About Live Feedback Participation

When you participate in Live Feedback, it collects relevant information for further improvement. For information on Live Feedback, see [Live Feedback Overview](#).

When you install NetWitness Suite, you will be prompted to participate in Live Feedback. For information, see [Configure Live Services Settings](#)

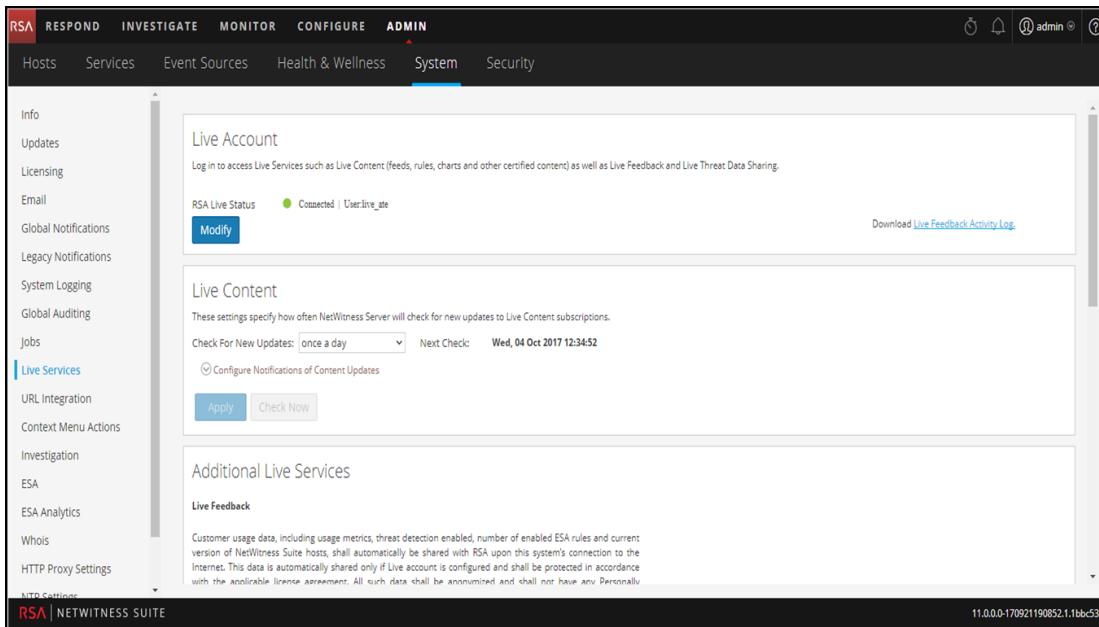
If needed, you can manually download historical usage data and share it with RSA. For information on how to download historical usage data and share it with RSA, see [Upload Data to RSA for Live Feedback](#).

This topic contains the following procedures:

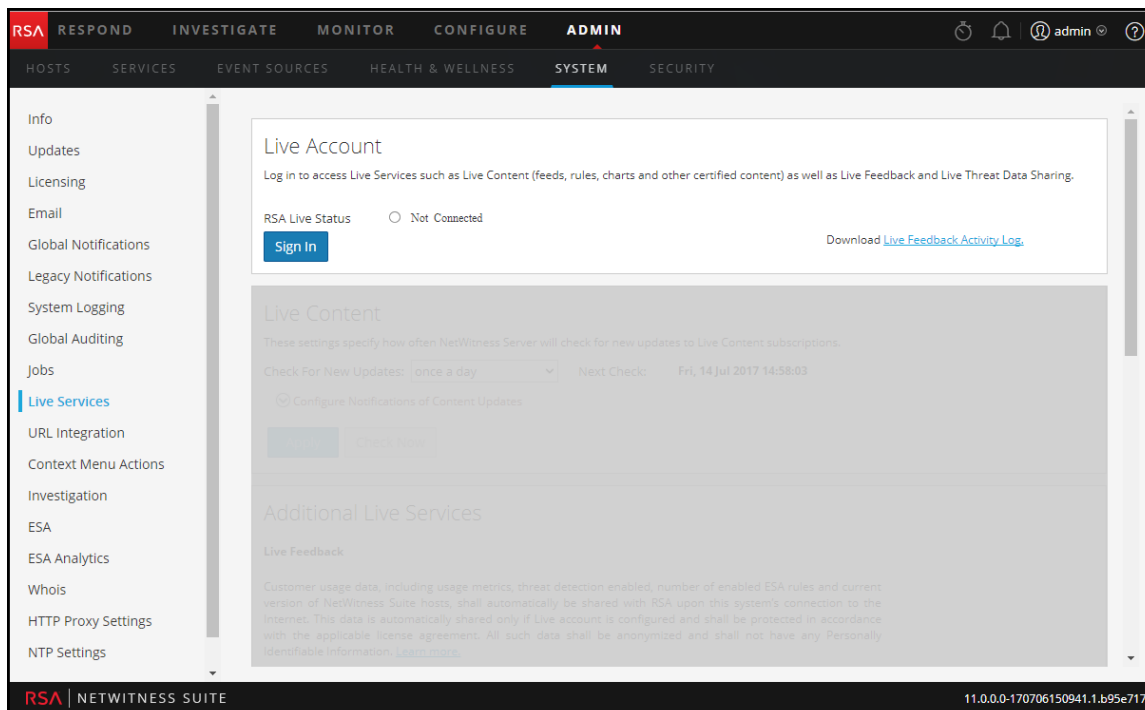
- [Access the Live Services Configuration Panel](#)
- [Configure Live Account](#)
- [Configure the Live Content Synchronization Interval and Notification](#)
- [Force Immediate Synchronization](#)
- [Using RSA Live Connect \(Beta\)](#)

## Access the Live Services Configuration Panel

1. Go to **ADMIN > System**.
2. In the option panel, select **Live Services**.



**Note:** If you are not signed in with your Live Account credentials, a masked screen is displayed.



## Configure Live Account

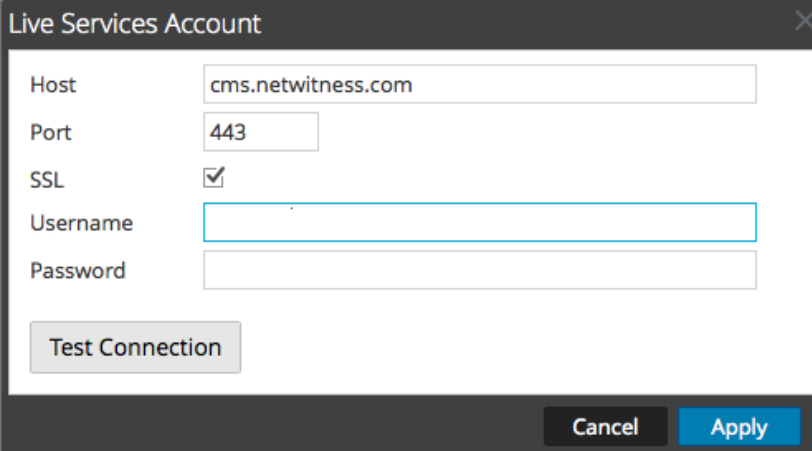
In the **Live Account** section, you must set up the user's Live account. The information needed to set up the user's Live account consists of the Username, Password, and Live URL for the Content Management System. This information is provided by Customer Care.

To configure a Live account:

1. In the **Live Account** section, click **Sign In**.

**Note:** The **Modify** button shows that the live account is configured. Click **Modify** to change the user that is accessing Live Services.

2. In the Live Services Account dialog box, enter the Host (typically **cms.netwitness.com**) and type your username and password.



The screenshot shows a dialog box titled "Live Services Account". It contains the following fields and controls:

- Host:** A text input field containing "cms.netwitness.com".
- Port:** A text input field containing "443".
- SSL:** A checkbox that is checked.
- Username:** An empty text input field.
- Password:** An empty text input field.
- Test Connection:** A button located below the Username and Password fields.
- Cancel:** A button at the bottom right.
- Apply:** A button at the bottom right, highlighted in blue.

3. (Optional) If you are using a different CMS, type the host URL for the Content Management System. The default points to the CMS at **cms.netwitness.com**.
4. (Optional) If you are using a different CMS, type the communications port for Live to send requests to the Content Management System. The default for this field is **443**, which is the communications port on the Content Management System.
5. (Optional) If you do not want to use SSL, uncheck the **SSL** option. (SSL is enabled by default.)
6. Click **Test connection** to test the connection to CMS.
7. To save and apply the configuration, click **Apply**.

## Configure the Live Content Synchronization Interval and Notification

You can change the interval at which NetWitness Suite checks for new updates to Live Content:

1. Use the **Check for New Updates** field to change the interval. Select an interval from the drop-down list. The default value for this setting is **once a day**.

### Live Content

These settings specify how often NetWitness Server will check for new updates to Live Content subscriptions.

Check For New Updates:  Next Check: Thu, 10 May 2017 08:00:00

[Configure Notifications of Content Updates](#)

E-Mail addresses specified here will receive messages containing a list of subscribed resources that have been updated in the last 24hrs.

Email Addresses

HTML Format

2. To configure Live Services to send update reports to one or more people, in the **Email Addresses** field, type the email addresses as a comma-separated list, for example, **john@company.com,ted@company.com,brian@company.com**
3. (Optional) To receive messages in HTML format rather than plain text, select **HTML Format**.
4. To save and apply, click **Apply**.

The time and date of the next scheduled Live synchronization based on the configured interval for checking is displayed.

### Force Immediate Synchronization

Instead of waiting for the next scheduled resource cycle, this option forces Live to begin immediate synchronization of the subscribed resources in this instance of NetWitness Suite. One use for this is to see the immediate impact of a configuration change. For example, a new service has been added, or new resources have been toggled for automatic deployment. The scheduled synchronization could take place hours later if Live Services is set to synchronize a few times a day.

**Caution:** Synchronization can cause a parser reload if a FlexParser is deployed in the update cycle. This is acceptable once or twice a day, but a number of back-to-back parser reloads can cause packet loss at the Decoder. If this is the initial setup and you haven't configured Live resource subscriptions, do not Synchronize Now. Wait until you have configured subscriptions.



To force immediate synchronization, click **Check Now**. NetWitness Suite checks for updates in subscribed resources.

### Using RSA Live Connect (Beta)

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

- Threat Insights
- Analyst Behaviors

#### Threat Insights

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

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

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

#### Analyst Behaviors

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

## Live Feedback Overview

This topic provides an introduction to Live Feedback. Live Feedback collects relevant information such as the Licensing usage data for Packet Decoder, Log Decoder and Malware Analysis, Threat Detection Enabled or Disabled status, Number of enabled ESA rules, and version number details of all the services of NetWitness Suite. For more information about the licensing usage data for Packer Decoder, Log Decoder and Malware Analysis, see the "Metered Licenses Tab" topic in the *Licensing Guide*. The information is collected to improve future releases of NetWitness Suite. You will automatically be signed on to live feedback and you cannot disable this option.

In addition to this, information on the Live Content Usage can also be shared with RSA. Live Content usage metrics for resource types from **CONFIGURE > Live Content > Search Criteria** such as total count of RSA Application Rule, RSA Correlation Rule etc. can be shared with RSA. The information collected is used to improve the use of Live Content. For more information about sharing live content configuration, see [Live Services Configuration Panel](#).

### About Live Feedback Participation

When you participate in Live Feedback, it collects relevant information for further improvement. For information on Live Feedback, see [Live Feedback Overview](#).

When you install NetWitness Suite, you will be prompted to participate in Live Feedback. For information, see [Configure Live Services Settings](#)

If needed, you can manually download historical usage data and share it with RSA. For information on how to download historical usage data and share it with RSA, see [Upload Data to RSA for Live Feedback](#).

**Note:** Live Feedback is activated only if you have configured your Live account.

The Live Feedback data is in JSON format as mentioned below. When you sign up with your Live Account credentials, a single encrypted JSON file is automatically uploaded to the RSA servers everyday.

### JSON File

The JSON file consists of usage data information for a component or a set of components. In case of a set of components with the same license id, the usage data for all the components is aggregated and represented as a component called Entitlement. However, even if there is a single component such as a log decoder or decoder, an Entitlement component will be generated and will display the usage data for a single component. This aggregation is for components namely log decoders, decoders or malware analysis.

**Note:** The version of Entitlement is always null as it is the aggregate for a license data.

For example, if there are three Decoders with the same license id "xxx" with the following usage data:

Decoder1 = 150 MB

Decoder2 = 250 MB

Decoder3 = 100 MB

The aggregated usage data of 500 MB is displayed.

This JSON file is described in the following sections:

- Components
- Metrics
- Other Product Details
- Sample

## Components

Details of each service in your NetWitness Suite deployment. This is represented as Component. For each component the following details are displayed.

Component	Description
Version	Version number of the component in the NetWitness Suite deployment. For example, 11.0.0.0.x.x.x.x.
ID	This is the unique Component ID that represents the host and is used to link to the metrics generated.
Properties	<ul style="list-style-type: none"><li>• <b>Name</b> - This is the name of the property for that component. For example, malware analysis, ESA, log decoder, etc.</li><li>• <b>Value</b> - This is the unique value to identify the component.</li></ul>

## Metrics

Metrics of the components (hosts) namely log decoder, decoder and malware analysis. The license usage data for each host is shared. For Live Content usage metrics, resource types from **Live > Search** such as total count of RSA Application Rule, RSA Correlation Rule etc. are shared.

Component	Description
StartTimeUTC	This is the time from when the metrics is collected. (in EPOCH format).

Component	Description
Stats	<ul style="list-style-type: none"> <li>• <b>Value</b> - This is the value generated for the specific component ID for each component.</li> <li>• <b>Name</b> - This is the name of the statistics for which the metrics is collected. For example, Capture Total Bytes.</li> </ul>
EndTimeUTC	This is the time when the metrics collection is complete (in EPOCH format).
Component ID	This is the ID of the component for which the value is recorded.

## Other Product Details

- **Product Type** - This is the name of the product. In this example, the Product Type is NetWitness Suite.
- **Version** - This is the version of the JSON file which tracks the changes made to the file format.
- **Product Instance** - This is the License Server ID.
- **Checksum** - This is the information which is used for integrity checks.

The following table describes details of the JSON file with examples.

Metrics	Description
Content	Displays the content that contains all the Components, Metrics, Product Type and Product Instance data except Checksum.

Metrics	Description
Components	<p>The details of all the services in NetWitness Suite are represented as a Component. The details of the component such as the version number of the component, the name, and the value is displayed as shown below:</p> <pre data-bbox="472 401 1281 751"> "Content": {   "Components": [{     "Version": "10.6.1.0",     "Id": 5,     "Properties": [{       "Value": "5714c78be4b0ea5bd2b96e63",       "Name": "InstanceId"     }],     "Name": "malwareanalysis"   }], }, </pre> <p><b>Version:</b> Displays the version of NetWitness Suite service. For example, 11.0.0.0.</p> <p><b>ID:</b> Displays an unique id which is generated for the NetWitness Suite service and is used to link to the metrics for that particular component. In this example, the ID for Malware Analysis is 5 and the metrics is displayed for ComponentId 5 in bytes, as shown below:</p> <pre data-bbox="472 1056 1015 1325"> "Metrics": [{   "StartTimeUTC": 1442102400000,   "Stats": [{     "Value": "1582940012678",     "Name": "Total FileBytes"   }],   "EndTimeUTC": 1442188799000,   "ComponentId": 5 }], }, </pre> <p><b>Properties:</b> Displays the properties for the component such as name and value as shown in the above figure.</p> <p><b>Value:</b> Displays the value of the property which is an internal UUID for a component as shown in the above figure This is generated by NetWitness Suite. For example, For malware analysis the value displayed as "55f7a0b30e502231c42d063f"</p> <p><b>Name: "InstanceId":</b> Displays the name of the property as shown in the above figure.</p> <p><b>Name": "malwareanalysis":</b> Displays the name of component which is a service name such as LogDecoder, Decoder, or MalwareAnalysis.</p>

Metrics	Description
Metrics	<p>Displays the list of the metrics with the usage data for components namely log decoder, decoder and malware analysis.</p> <p>In this example, the metrics is displayed for ComponentId 5 in bytes, as shown below.</p> <pre data-bbox="375 464 922 737"> "Metrics": [{   "StartTimeUTC": 1442102400000,   "Stats": [{     "Value": "1582940012678",     "Name": "Total FileBytes"   }],   "EndTimeUTC": 1442188799000,   "ComponentId": 5 }], </pre> <p><b>StartTimeUTC:</b> Displays the time when the metrics is collected, in the EPOCH format.</p> <p><b>Stats:</b> Displays the usage value and usage type statistics of the component.</p> <p><b>Value:</b> Displays the value of the statistics. For example, "Value": "1582940012678" as shown in the above figure.</p> <p><b>Name:</b> Displays the name of the statistics. For example, Capture Total Bytes or Total File bytes.</p> <p><b>EndTimeUTC:</b> Displays the time when the metrics collection is complete, in the EPOCH format.</p> <p><b>ComponentId:</b> Displays the component id for which the metric values are collected. This is the same as the "ID" in the Components section.</p>
Content	<p>Displays the content that contains all the Components, Metrics, Product Type and Product Instance data except Checksum.</p>

Metrics	Description
---------	-------------

**Components** The details of all the services in NetWitness Suite are represented as a Component. The details of the component such as the version number of the component, the name, and the value is displayed as shown below:

```

"Content": {
  "Components": [{
    "Version": "10.6.2.0",
    "Id": 6,
    "Properties": [{
      "Value": "57444ddde4b0dd618093064d",
      "Name": "InstanceId"
    }],
    "Name": "reportingengine"
  }],
},

```

**Version:** Displays the version of NetWitness Suite service. For example, 11.0.0.0

**ID:** Displays an unique id which is generated for the NetWitness Suite service and is used to link to the metrics for that particular component. In this example, the ID for Reporting Engine is 6 and the metrics is displayed for ComponentId 6 in Total Count, as shown below:

```

"Metrics": [{
  "StartTimeUTC": 1473292800000,
  "Stats": [{
    "Value": "10",
    "Name": "Number of RE Report"
  },
  {
    "Value": "2",
    "Name": "Number of RE Alert"
  },
  {
    "Value": "1",
    "Name": "Number of RE Chart"
  },
  {
    "Value": "14",
    "Name": "Number of RE Rule"
  },
  {
    "Value": "2",
    "Name": "Number of Enabled RE Alert"
  },
  {
    "Value": "1",
    "Name": "Number of Enabled RE Chart"
  }
  ],
  "EndTimeUTC": 1473379199000,
  "ComponentId": 6
},
],

```

**Metrics****Description**

**Properties:** Displays the properties for the component such as name and value as shown in the above figure.

**Value:** Displays the value of the property which is an internal UUID for a component as shown in the above figure. This is generated by NetWitness Suite. For example, for Reporting Engine the value displayed as "57444ddde4b0dd618093064d"

**Name: "InstanceId":** Displays the name of the property as shown in the above figure.

**Name": "reportingengine":** Displays the name of component which is a service name such as LogDecoder, Decoder, or ReportingEngine.

**Name:** Displays the list of the metrics with the usage data for components namely log decoder, decoder and reportingengine.

In this example, the metrics is displayed for ComponentId 6 in bytes, as shown below.

```
"Metrics": [{
  "StartTimeUTC": 1473292800000,
  "Stats": [{
    "Value": "10",
    "Name": "Number of RE Report"
  },
  {
    "Value": "2",
    "Name": "Number of RE Alert"
  },
  {
    "Value": "1",
    "Name": "Number of RE Chart"
  },
  {
    "Value": "14",
    "Name": "Number of RE Rule"
  },
  {
    "Value": "2",
    "Name": "Number of Enabled RE Alert"
  },
  {
    "Value": "1",
    "Name": "Number of Enabled RE Chart"
  }
  ]],
  "EndTimeUTC": 1473379199000,
  "ComponentId": 6
},
```

**StartTimeUTC:** Displays the time when the metrics is collected, in the EPOCH format.



Metrics	Description
	<p><b>Stats:</b> Displays the usage value and usage type statistics of the component.</p> <p><b>Value:</b> Displays the value of the statistics. For example, Number of RE Report is 10, Number of RE Alert is 2, Number of RE chart is 1 etc as shown in the above figure.</p> <p><b>Name:</b> Displays the name of the statistics. For example, Number of RE Report, Number of RE Alert, Number of RE chart, Number of RE Rule, Number of Enabled RE Alert, Number of Enabled RE Chart.</p> <p><b>EndTimeUTC:</b> Displays the time when the metrics collection is complete, in the EPOCH format.</p> <p><b>ComponentId:</b> Displays the component id for which the metric values are collected. This is the same as the "ID" in the Components section.</p>
ProductType	Displays the product type that generates the file. For example, <pre>"ProductType": "NetWitness Suite"</pre>
ProductInstance	Displays the License server Id and is unique per NetWitness Suite. For example, <pre>"ProductInstance": "00-0C-29-6C-66-E3"</pre>
Checksum	Displays the Checksum for the "Content" section in the file. Used by RSA for integrity check. For example, <pre>"Checksum": "883DACF97E4BCD9F590A1461A4DD0A312B5883A6CF82E0518E77AAB6A6DDB654"</pre>

### Sample

Here is a sample JSON file.

```
{
  "Content": {
    "Components": [{
      "Version": "10.6.1.0",
      "Id": 7,
      "Properties": [{
        "Value": "57470c96e4b0cf62c7bfbfd53",
        "Name": "InstanceId"
      }],
      "Name": "esa"
    },
    {
      "Version": "10.6.1.0",
      "Id": 4,
      "Properties": [{
        "Value": "5714c78be4b0ea5bd2b96e69",
        "Name": "InstanceId"
      }],
      "Name": "incidentmanagement"
    },
    {
      "Version": "10.6.1.0",
      "Id": 2,
      "Properties": [{
        "Value": "5714c78be4b0ea5bd2b96e65",
        "Name": "InstanceId"
      }],
      "Name": "sa"
    },
    {
      "Version": "10.6.1.0",
      "Id": 1,
      "Properties": [{
        "Value": "5714c78be4b0ea5bd2b96e63",
        "Name": "InstanceId"
      }],
      "Name": "malwareanalysis"
    },
    {
      "Version": "10.6.1.0",
      "Id": 3,
      "Properties": [{
        "Value": "5714c78be4b0ea5bd2b96e67",
        "Name": "InstanceId"
      }],
      "Name": "reportingengine"
    }
  ],
  "Metrics": [{
    "StartTimeUTC": 1464480000000,
    "Stats": [{
      "Value": "Disabled",
      "Name": "Threat Detection"
    }],
    {
      "Value": "3.0",
      "Name": "Number Of Enabled ESA Rules"
    }
  ],
  "EndTimeUTC": 1464566399000,
  "ComponentId": 7
}],
  "EndTime": 1464566399000,
  "Version": "1.0",
  "StartTime": 1464479999000,
  "ProductType": "Security Analytics",
  "ProductInstance": "00-0C-29-A2-57-B4"
},
  "Checksum": "6445C704D3F9E67D24DBA8F11EB6C003CBCC0E199576342E6E6D2545524F583F"
}
```

## Upload Data to RSA for Live Feedback

This topic provides instructions for a NetWitness Suite administrator to export the metrics in NetWitness Suite for Live Feedback.

If the Live Account is not configured, you can manually upload the usage data to RSA. For more information, see [Live Services Configuration Panel](#).

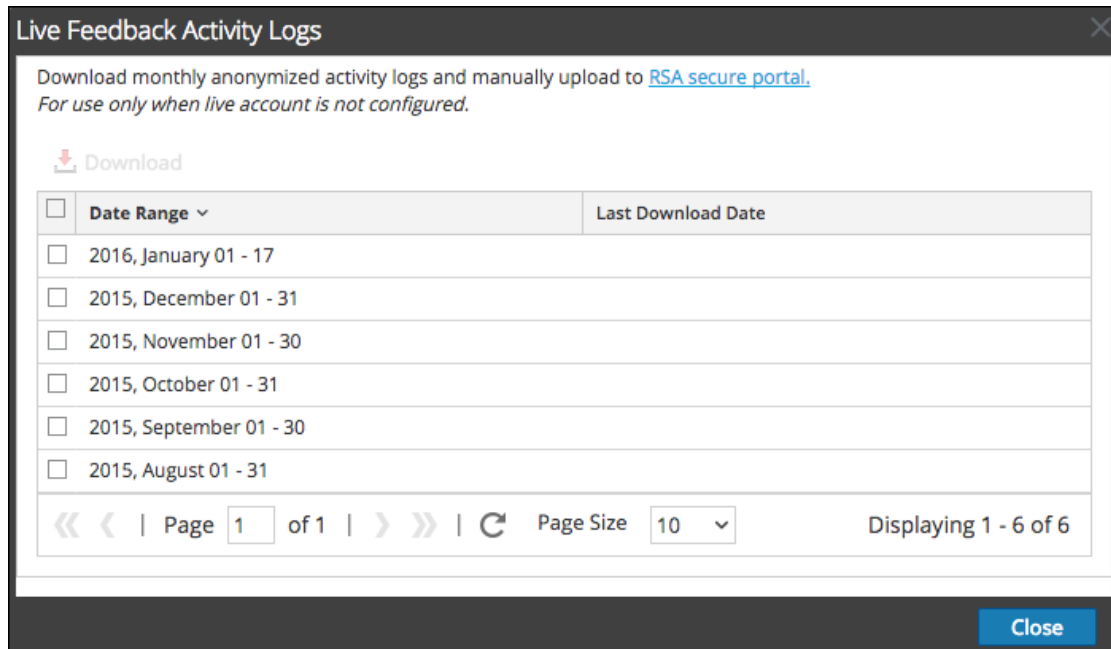
The Live Account section has a Live Feedback Activity Log which enables you to download the usage data required for Live Feedback. This is active regardless of the Live Account configuration.

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

### Download Live Feedback Historical Data

To download the Live Feedback historical data:

1. Go to **ADMIN > System**.
2. In the options panel, select **Live Services**.  
The **Live Account** screen is displayed which consists of the **RSA Live Status** and **Download Live Feedback Activity Log**.
3. Click the **Download Live Feedback Activity Log**.  
The **Download Live Feedback Activity Log** window opens which allows the NetWitness Suite user to download the required Live Feedback historical data.



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

**Note:** If you select multiple entries in the history table, the downloaded zip file consists of an individual JSON file for each month.

The downloaded Live Feedback data is in JSON format, and is bundled as a .zip file. For more information, see [Live Feedback Overview](#).

### Share Data with RSA

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

To share the data to RSA:

1. Click on the **RSA Secure Portal** available on the **Live Feedback Activity Logs** window. The RSA NetWitness® Suite Live Feedback login screen is displayed.
2. Login to the Upload Live Feedback Activity Logs portal using your Live ID credentials.
3. Click **Choose File**, and select the downloaded file.
4. Click **Upload**.

## Configure Log File Settings

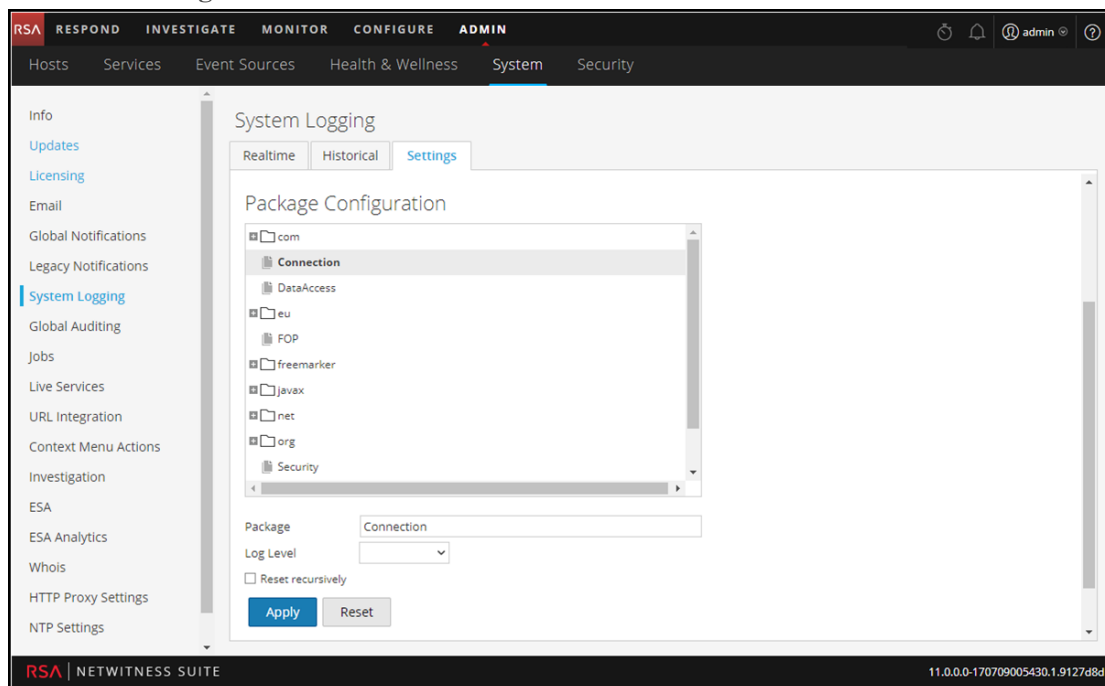
In RSA NetWitness® Suite, you can configure the size of the log files, the number of backup log files maintained, as well as the default logging levels for the packages within NetWitness Suite.

### Configure System Log File Size and Backup Count

The log file size and backup count are configured with default values. If you want to change the default values for the log file size and number of backups:

1. Go to **ADMIN > System**.
2. In options panel, select **System Logging**.

The System Logging Configuration panel opens to the Realtime tab by default.

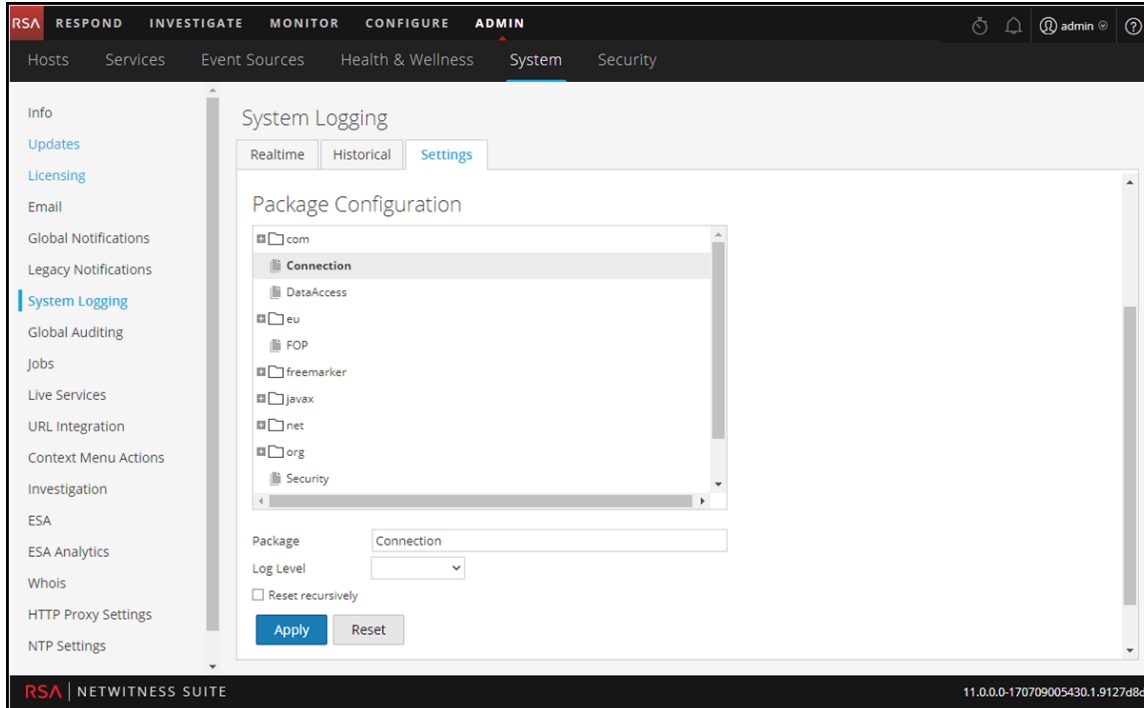
3. Click the **Settings** tab.

4. In the **Max Log Size** field, type the maximum size in bytes. The minimum value for this setting is **4096**.
5. In the **Max # Backup Files** field, type the maximum number of backup logs to maintain. The minimum value for this setting is **0**. When the maximum number of log files is attained, and a new backup file is made, the oldest backup is discarded.
6. Click **Apply**.  
The changes go into effect immediately.

### Set the Log Level for an Individual Package

The Package Configuration section shows the NetWitness Packets in a tree structure. The tree contains all the packages used within NetWitness Suite. You can drill down into the tree to view the log levels of each package. The log level for all packages that are not explicitly set is the same as the **root** log level. To set the log level for a package:

1. Select the package in the **Package** tree.  
The name of the package is displayed in the **Package** field. If a log level is already set for the package, that level is shown.



2. Select the **Log Level** in the drop-down list.
3. Click **Apply**.  
The new log level becomes effective immediately.
4. (Optional) If you want to revert to the default log level specified for **root**, click **Reset**.

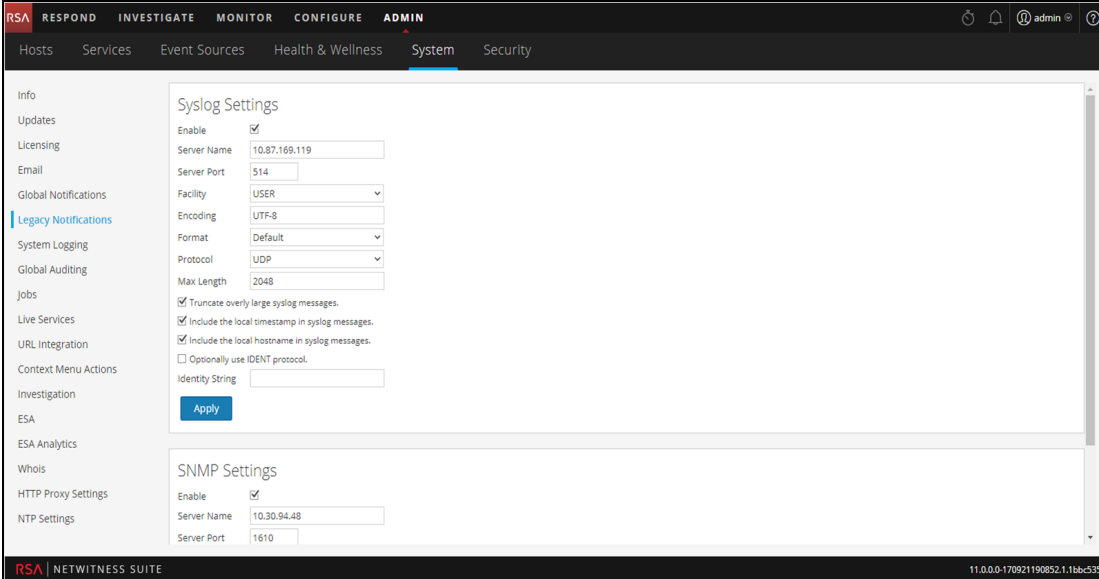
## Configure Syslog and SNMP Settings

On the Legacy Notifications panel, you can configure syslog and SNMP notification settings. These configurations are used for Entitlement, legacy Event Source Management (ESM), Warehouse Connector monitoring, and Archiver monitoring.

### Configure and Enable Syslog Settings

1. Go to **ADMIN > System**.

- In the options panel, select **Legacy Notifications**.  
The Legacy Notifications Configuration panel is displayed.



The screenshot shows the RSA NetWitness Suite configuration interface. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The 'ADMIN' section is active, and the 'System' sub-section is selected. The left sidebar lists various configuration categories, with 'Legacy Notifications' highlighted. The main content area is divided into two sections: 'Syslog Settings' and 'SNMP Settings'. The 'Syslog Settings' section includes an 'Enable' checkbox (checked), 'Server Name' (10.87.169.119), 'Server Port' (514), 'Facility' (USER), 'Encoding' (UTF-8), 'Format' (Default), 'Protocol' (UDP), and 'Max Length' (2048). There are also three checked options: 'Truncate overly large syslog messages', 'Include the local timestamp in syslog messages', and 'Include the local hostname in syslog messages'. An unchecked option 'Optionally use IDENT protocol' is also present, along with an 'Identity String' field. An 'Apply' button is located below the Syslog settings. The 'SNMP Settings' section includes an 'Enable' checkbox (checked), 'Server Name' (10.30.94.48), and 'Server Port' (1610). The bottom of the interface shows the 'RSA | NETWITNESS SUITE' logo and the version number '11.0.0-170921190852.1.1bc535'.

- In the **Server Name** and **Server Port** fields under **Syslog Settings**, type the host name where the target syslog process is running and the port where the target syslog process is listening.
- In the **Facility**, **Encoding**, **Format**, and **Max length** fields, specify the syslog facility, message text encoding, message format, and maximum message length.
- In the **Protocol** field, select either UDP or TCP.
- (Optional) Select the options for what to include in messages: **Truncate overly large syslog messages**, **Include the local timestamp in syslog messages**, and **Include the local hostname in syslog messages**.
- (Optional) Configure syslog to prepend an Identity String before each syslog alert.
- Click the **Enable** checkbox.
- Click **Apply**.  
Syslog notifications are immediately enabled.

[Legacy Notifications Configuration Panel](#) provides detailed information about these settings.

## Configure and Enable SNMP Settings

- Go to **ADMIN > System**.
- In the options panel, select **Legacy Notifications**.  
The Legacy Notifications Configuration panel is displayed, with SNMP Settings at the

bottom of the panel.



3. In the **Server Name** and **Server Port** fields under **SNMP Settings**, type the host name and listening port of the SNMP trap host.
4. Select the **SNMP version** in the drop-down menu, **v1** or **v2c**.
5. In the **Trap OID** field, specify the object ID for the SNMP trap on the trap host that receives the audit event. The default value is **0.0.0.0.1**.
6. In the **Community** field, specify the community string used to authenticate on the SNMP trap host, the default value is **public**.
7. Click the **Enable** checkbox.
8. Click **Apply**.  
SNMP notifications are immediately enabled.

[Legacy Notifications Configuration Panel](#) provides detailed information about these settings.

## Disable Syslog or SNMP Settings

To disable syslog or SNMP settings on this NetWitness Suite instance:

1. Clear the appropriate **Enable** checkbox.
2. Click **Apply**.  
The selected settings are immediately disabled.



## Additional Procedures

---

Additional procedures are not essential for the set up of NetWitness Suite, they include certain customization options that are beyond the usual setup; for example, adding custom context menus or setting up a proxy.

[Add Custom Context Menu Actions](#)

[Configure NTP Servers](#)

[Configure Proxy for NetWitness Suite](#)

[Add New Configuration Dialog](#)

[Supported CEF Meta Keys](#)

[Supported Global Audit Logging Meta Key Variables](#)

[Global Audit Logging Operation Reference](#)

[Local Audit Log Locations](#)

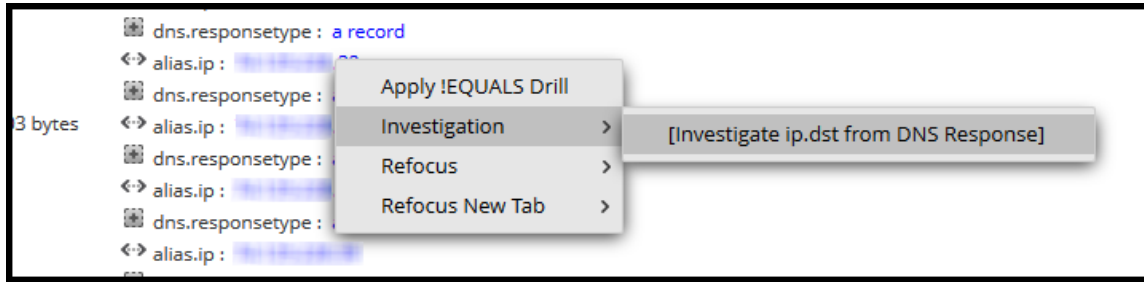
### Add Custom Context Menu Actions

In the Context Menu Actions panel, administrators can view, add, and edit context menu actions for the current instance of NetWitness Suite. Each context menu action applies to a specific context in the NetWitness Suite user interface, and appears as an option when you right-click a specific location in the user interface.

Some context menu actions are built into NetWitness Suite; you cannot edit or delete any of the default context menu actions. You can create and edit custom context menu actions. If you want to create a custom variation of a built-in context menu action, you can copy the configuration to a new context menu action and modify the custom context menu action. A context menu action is defined by cascading style sheet (CSS) code that defines:

- The title of the option in the context menu.
- The NetWitness Suite module in which the context menu is available.
- The content to which the action applies.

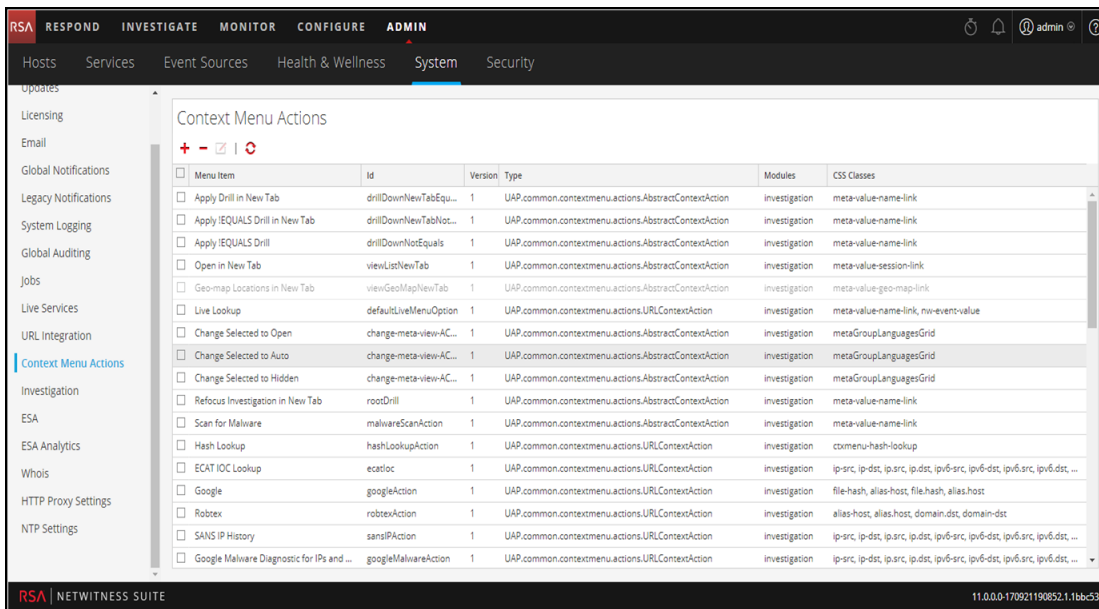
This is an example of a custom context menu action; the steps and CSS code to create this example are provided as an example procedure below.



## View Context Menu Actions in NetWitness Suite

To view existing context actions in NetWitness Suite both default and custom:

1. Go to **ADMIN > System**.
2. In the options panel, select **Context Menu Actions**.

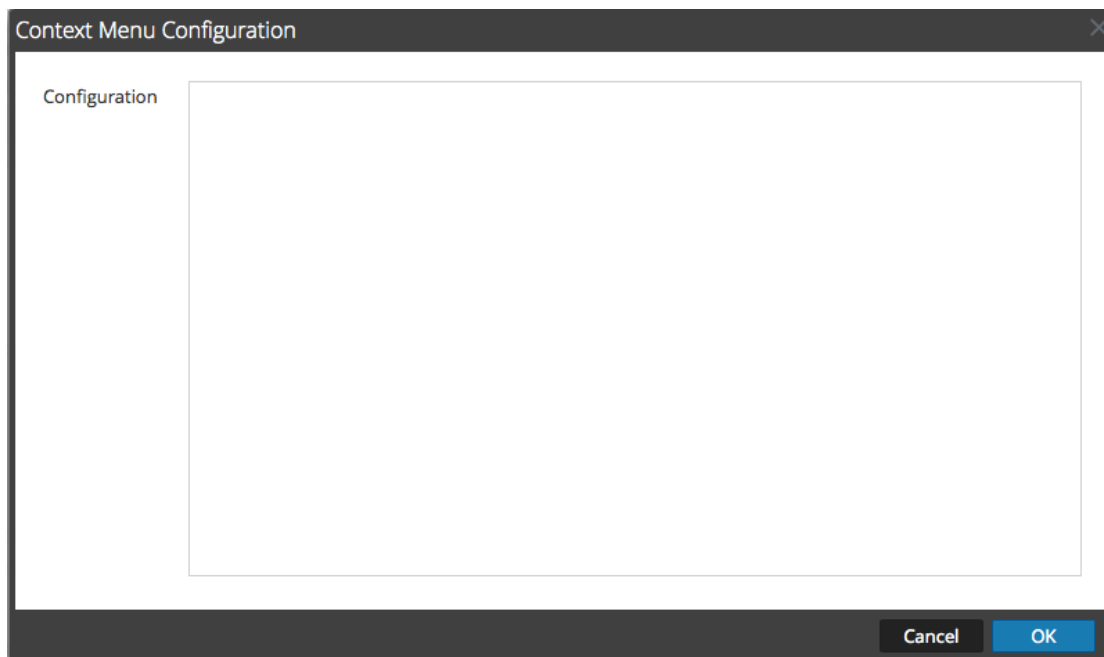


Details of the information in the Context Menu Action panel are provided in [Context Menu Actions Panel](#).

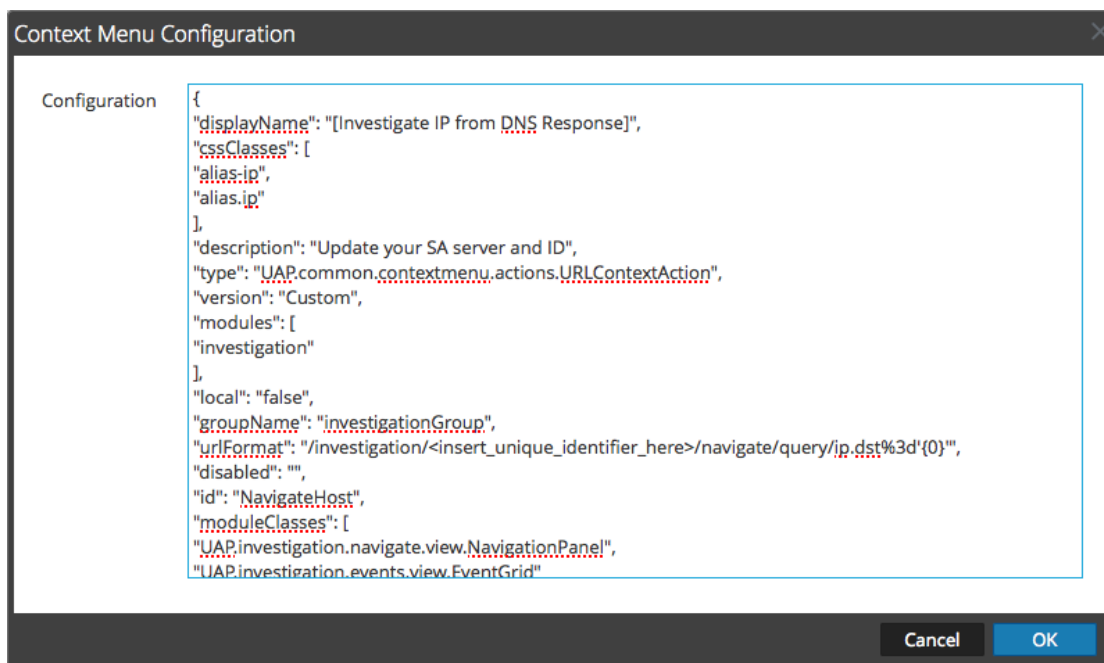
## Add a Context Menu Action

To add a context menu action in NetWitness Suite:

1. In the toolbar, click **+**.  
The Context Menu Configuration dialog is displayed.



2. Type the CSS code to define the context menu action. The example procedure at the end of this topic provides step-by-step instructions that you can use to create a useful context menu action.



3. Click **OK**.

The new context menu action is created and added at the end of the list of context menu actions.

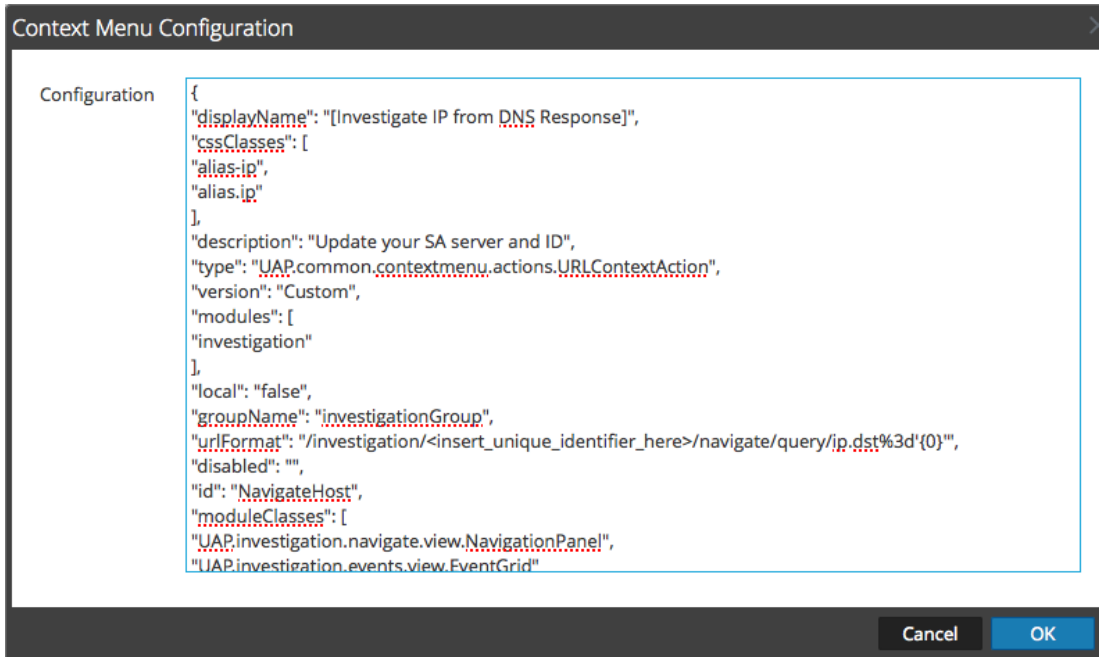
- To activate the new context menu action, restart the browser.  
The context menu action becomes available in the configured location.

### Edit a Context Action

To edit a context action:

- Select the row in the grid and either **double-click** the row or click .


The **Context Menu Configuration Dialog** is displayed.



- Edit the **Configuration**.
- To save the changes, click **OK**.
- To use the updated action, restart the browser.

### Delete a Context Action

To remove a context menu action from NetWitness Suite entirely:

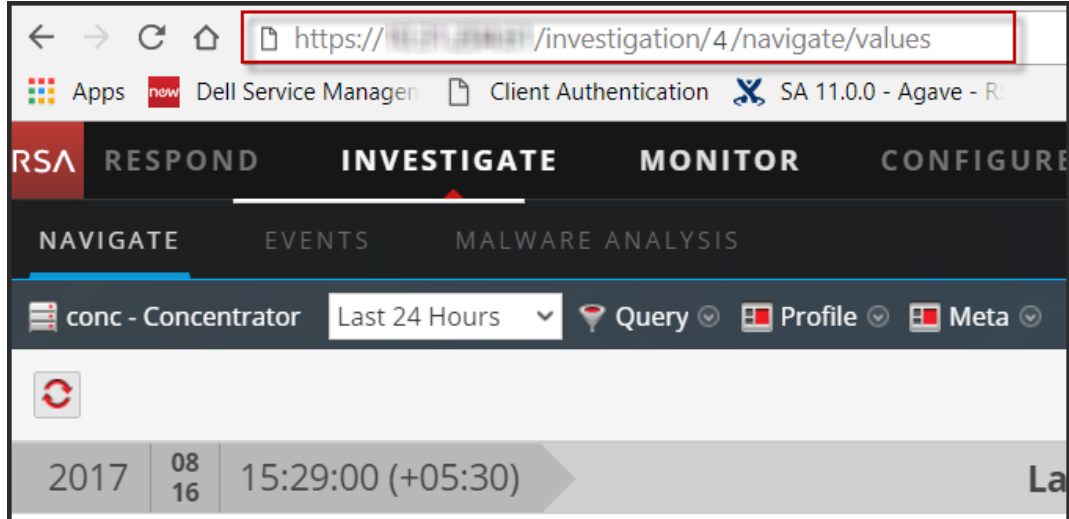
- Select the action.
- Click .
- A dialog requests confirmation that you want to delete the context menu action.
- Click **Yes**.  
The option is removed from the Context Menu Actions panel.
- Restart the browser to remove the action from the context menus in which it appeared.

## Example Procedure: Context Menu Action to Investigate ip.dst from alias.ip

This example adds a context menu action that allows analysts to pivot from the `alias.ip` values (the IP addresses returned from a DNS request) to the `ip.dst` meta key. It helps analysts to locate any detected traffic to the IP address that was returned for a DNS query.

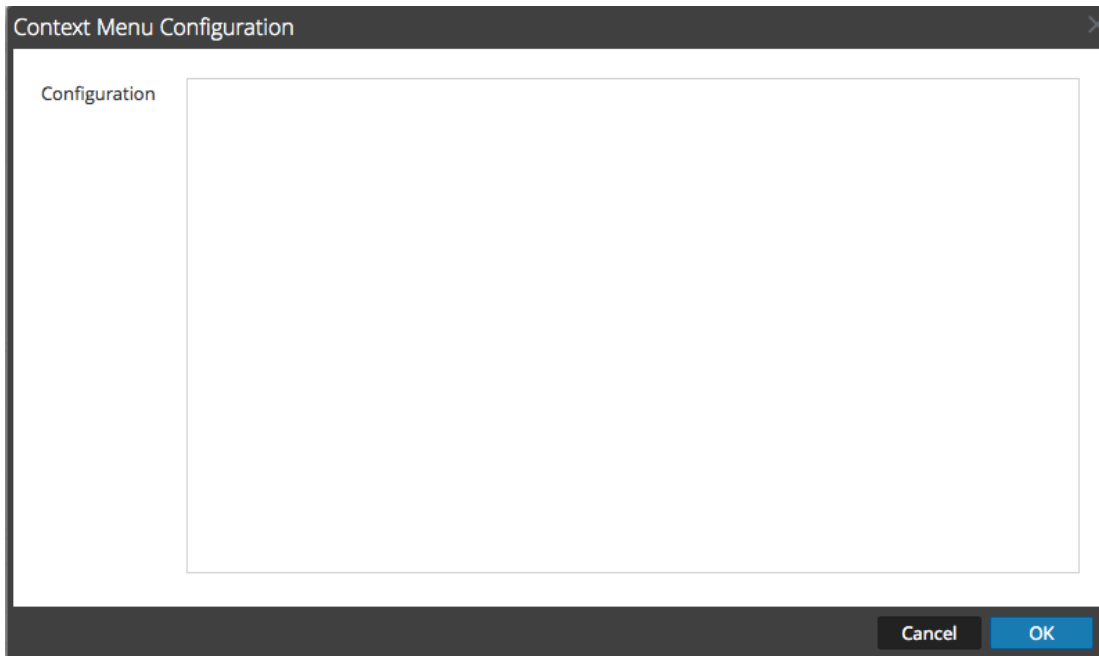
To implement the context menu action:

1. Determine the unique identifier for your NetWitness Server as follows:
  - a. Log onto NetWitness Suite, in the main menu, select **INVESTIGATE** > **Navigate**, choose a service (for example, a Concentrator) to investigate, and wait for the values to load.
  - b. Look for the URL and locate the number after `investigation`. In this example, the unique identifier for the action is 4. You need this unique identifier to add to the context menu action.



- In the toolbar, click **+**.

The Context Menu Configuration dialog is displayed.



- Copy the entire sample code block below and paste it in the window.

```
{
  "displayName": "[Investigate IP from DNS Response]",
  "cssClasses": [
    "alias-ip",
    "alias.ip"
  ],
  "description": "Update your NW server and ID",
  "type": "UAP.common.contextmenu.actions.URLContextAction",
  "version": "Custom",
  "modules": [
    "investigation"
  ],
  "local": "false",
  "groupName": "investigationGroup",
  "urlFormat": "/investigation/<insert_unique_identifier_
here>/navigate/query/ip.dst%3d'{0}'",
  "disabled": "",
  "id": "NavigateHost",
  "moduleClasses": [
```

```

        "UAP.investigation.navigate.view.NavigationPanel",
        "UAP.investigation.events.view.EventGrid"
    ],
    "openInNewTab": "true"
}

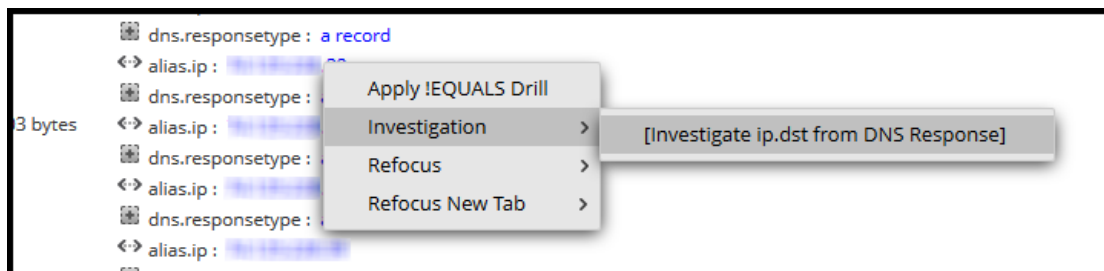
```

- In the **urlFormat** line replace **<insert-unique\_identifier\_here>** with your unique identifier. The URL should look like this:

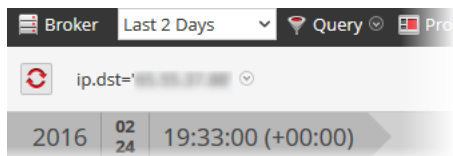
```
"/investigation/4/navigate/query/ip.dst%3d'{0}'"
```

- Click **OK**, and restart your browser.
- To test the action, open an investigation in the Navigate view and right-click on the meta key `alias.ip`.

The context menu with the Investigation option should look like the following figure.



- Should produce a pivot like this.



- If you are using this example for DNS traffic investigation, you may want to consider creating a meta group specific to DNS traffic as described in "Manage User-Defined Meta Groups" in the *Investigation and Malware Analysis Guide*.

## Configure NTP Servers

This topic provides instructions on how to configure Network Time Protocol (NTP) servers. NTP is a protocol designed to synchronize host machine clocks over a network. For more information on NTP go to their home page (<http://www.ntp.org/>).

**Note:** NW Core hosts must be able to communicate with the NW host with UDP port 123 for NTP time synchronization.

You use the **ADMIN > System > NTP Settings** view to configure one or more NTP servers. After you configure an NTP server, NetWitness Suite uses NTP to synchronize the host machine clocks. You configure multiple NTP servers for Fail Over purposes. This topic contains the following procedures:

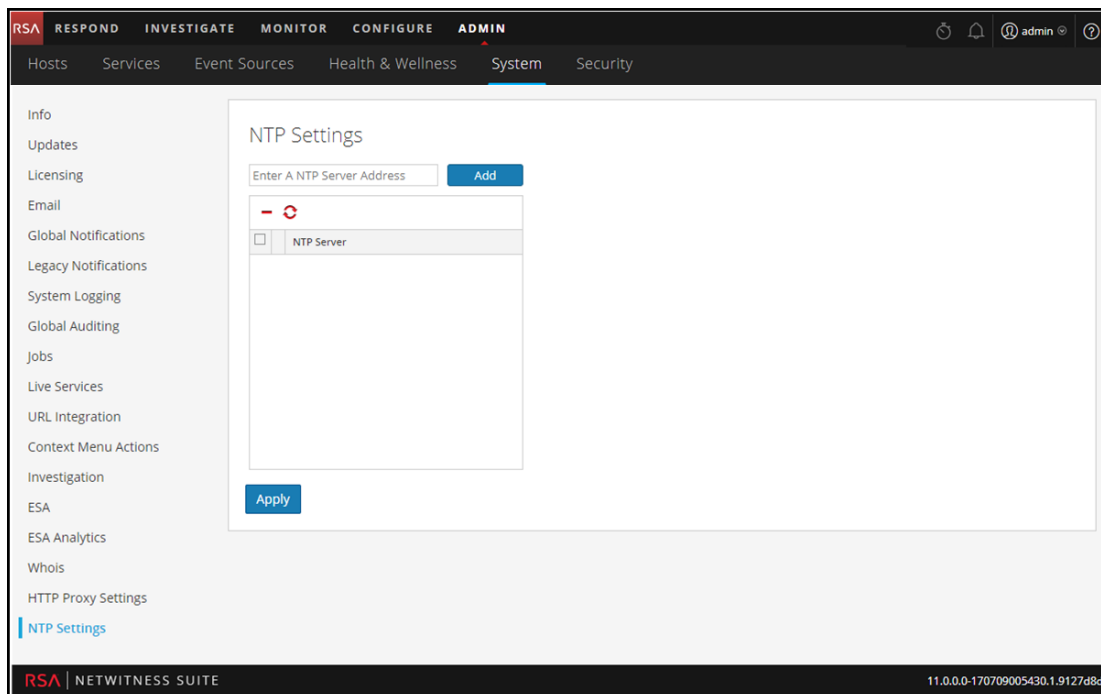
- Add an NTP Server
- Modify an NTP Server

## Add an NTP Server

To add an NTP server:

1. Go to **ADMIN > System**.
2. In the options panel, select **NTP Settings**.

The NTP Settings panel is displayed prompting you to enter the hostname (that is, the IP Address or FQDN) of an NTP server.



3. Enter the IP address or FQDN for an NTP server.  
If the hostname syntax is invalid, NetWitness Suite disables the **Add** and **Apply** buttons and displays **Entered an invalid hostname**.
4. Click **Add**.
  - If the hostname syntax is valid and NetWitness Suite can reach the server, it displays **Validating**.



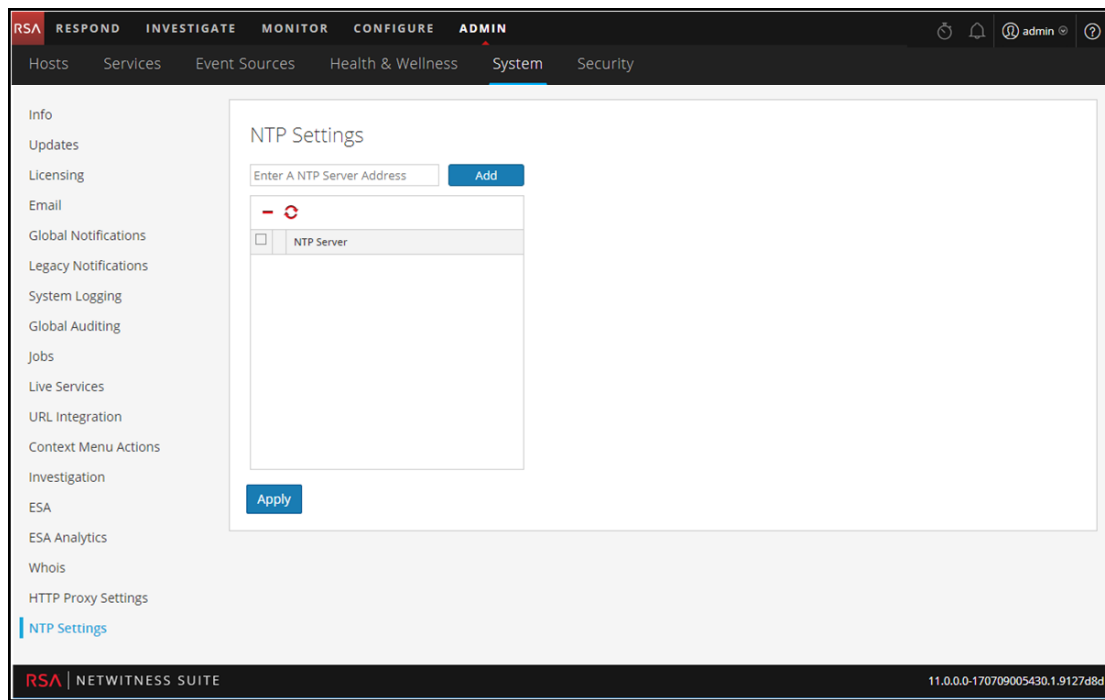
- If the hostname syntax is valid and NetWitness Suite cannot reach a server, the following is displayed, where *hostname* is the hostname that you attempted to add: **The NTP server *hostname* is unreachable. Please verify the address or check your firewall settings.**
5. Click **Apply**.  
A dialog displays notification that the settings have been saved and requests confirmation that you want to apply the settings now.
  6. Click **Yes**.  
The NTP server specified now ensures that your host machine clocks are synchronized. If you decide to configure multiple NTP servers and a server is down, NetWitness Suite will fail over to next server configured.

For details of the parameters and descriptions, see [NTP Settings Panel](#).

## Modify an NTP Server

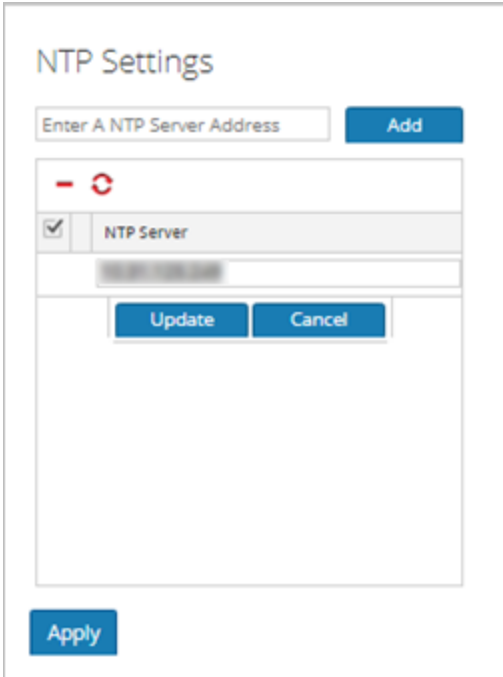
To modify an existing NTP server:

1. Go to **ADMIN > System**.
2. In the options panel, select **NTP Settings**.  
The NTP Setting panel is displayed.



3. Double-click the **NTP Server** hostname that you want to modify.

The NTP Server textbox becomes editable and the Update and Cancel buttons are displayed.



The screenshot shows the 'NTP Settings' dialog box. At the top, there is a text input field labeled 'Enter A NTP Server Address' and an 'Add' button. Below this is a list of NTP servers. The first entry is 'NTP Server', which is highlighted in grey. A checkmark is visible to the left of the entry. Below the list, there is a text input field for editing the hostname, and two buttons: 'Update' and 'Cancel'. At the bottom of the dialog box, there is an 'Apply' button.

4. Edit the hostname, click **Update**, and click **Apply**. (click **Cancel** before you click **Apply** to cancel the edit.)

NetWitness Suite changes the hostname according to your edits.

## Add New Configuration Dialog

In the RSA NetWitness® Suite Administration System view Global Audit Logging Configurations panel, you can create multiple global audit logging configurations. These configurations are used to forward global audit logs to a central location to perform user audits.

Procedures related to global audit logging are described in [Configure Global Audit Logging](#).

To access the **Add New Configuration** dialog:

1. In the main menu, select **ADMIN > System**.
2. In the options panel, select **Global Auditing**.
3. In the **Global Audit Logging Configurations** panel, click **+**.

The **Add New Configuration** dialog is displayed.

**Add New Configuration**

Audit logs will be forwarded to the selected Notification Server with the selected Template.

The audit logs contain some of these user actions:  
User login success, User login failure, User logouts, Maximum login failures exceeded, All UI pages accessed, Committed configuration changes, Queries performed by the user, User access denied, Data export operations

Notification Servers and Templates [view settings](#)

Configuration Name:

Notifications: Notification Server:  Notification Template:

The Notifications section enables you to select a syslog notification server for the global audit logging configuration and a template to use for the global audit logs. The template defines the details of the global audit log entries.

## Features

The following table describes the features in the Add New Configuration and Edit Configuration dialogs.

Feature	Description
Notifications Servers and Templates <b>view settings</b> link	Takes you to the Global Notifications panel where you can view or configure the notification server and template settings. A syslog notification server and an audit logging template are required before you can create a global audit configuration.
Configuration Name	Specifies the unique name used to identify the global audit logging configuration.
Notification Server	Specifies the syslog notification server to send the selected audit log information. <a href="#">Configure a Destination to Receive Global Audit Logs</a> provides instructions on how to create a Syslog Notification Server for global audit logging.
Notification Template	Specifies the template to use for the global audit logging configuration. The template should be an Audit Logging template. For Log Decoders, use the <b>Default Audit CEF Template</b> . You can add or remove fields from the Common Event Format (CEF) template if you have specific requirements. <a href="#">Define a Template for Global Audit Logging</a> provides instructions. For third-party syslog servers, you can use a default audit logging template or define your own format (CEF or non-CEF). <a href="#">Define a Template for Global Audit Logging</a> provides instructions and <a href="#">Supported Global Audit Logging Meta Key Variables</a> describes the available variables.
<b>Reset Form</b> button	Clears the configuration settings in the dialog.

## User Actions Logged

The following table provides examples of some of the user actions logged from NetWitness Suite. These actions are the minimum user actions logged when applicable.

User Action	Example
User login success	A user logs on with valid credentials.
User login failure	A user tries to log on using invalid credentials.
User logouts	A user logs out from NetWitness Suite (Administration > Sign Out) or a user logs out due to a session timeout.
Max login failures exceeded	A user tries to log on using invalid credentials five times. Five (5) is the number of Max Login Failures defined in Administration Security view > Settings tab (Administration > Security > Settings tab).
All UI pages accessed	When a user accesses the Reporting module (Administration > Reports), it logs as [REP] Reports. When a user accesses the Administration System view (Administration > System), it logs as [ADM] System.
Committed configuration changes	A user changes his or her password and or any security setting (Administration > Security > Settings tab).
Queries performed by the user	A user performs an investigation query.
User access denied	A user tries to access a module and does not have permissions to access it.
Data export operations	A user exports data from the Events view (Investigation > Events > Actions > Export).

For lists of message type being logged by the various NetWitness Suite components, see [Global Audit Logging Operation Reference](#).



## Troubleshooting System Configuration

---

The topics in this section provide troubleshooting information for administrators who are configuring settings that apply across the system in NetWitness Suite.

[Troubleshoot Global Audit Logging](#)

[Troubleshooting NTP Server Configuration](#)

### Troubleshoot Global Audit Logging

This topic provides information about possible issues that NetWitness Suite users may encounter when implementing Global Audit Logging in NetWitness Suite. Look for explanations and solutions in this topic.


After you configure Global Audit Logging, you should test your audit logs to ensure that they show the audit events as defined in your audit logging template. If you cannot view the audit logs on your third-party syslog server or Log Decoder, or the audit logs do not appear as expected, look at the basic troubleshooting suggestions below. If you are still having issues, you can look at the advanced troubleshooting suggestions.

### Basic Troubleshooting

If you cannot view audit logs on a third-party syslog server or Log Decoder:

- Verify that RabbitMQ is up and running.
- Verify the syslog notification server configuration and make sure it is enabled.  
(This configuration is located at ADMIN > System > Global Notifications. Do not select Legacy Notifications.)
- Check the Global Audit Logging configuration.

[Configure Global Audit Logging](#) and [Verify Global Audit Logs](#) provide instructions. If you are sending audit logs to a Log Decoder:

- Ensure that the Log Decoder is aggregating on the Concentrator on the same host (ADMIN > Services > (Select Concentrator) >  > View > Config).
- Verify that the latest CEF parser is deployed and enabled.
- Check the audit logging notification template. You must use a CEF template and all logs feeding into the Log Decoder must use a CEF template.

If you are sending audit logs to a third-party syslog server:

- Ensure that the destination port configured for the third-party syslog server is not blocked by a firewall.

## Advanced Troubleshooting

In order to use Global Audit Logging on your network, RabbitMQ must be functioning.

For centralized audit logging, each of the NetWitness Suite services writes audit logs to rsyslog listening on port 50514 using UDP on the local host. The rsyslog plugin provided in the audit logging package adds additional information and uploads these logs to RabbitMQ.

Logstash running on the NetWitness Serverhost aggregates audit logs from all of the NetWitness Suite services, converts them to the required format, and sends them to a third-party syslog server or Log Decoder for investigation. You configure the format of the global audit logs and the destination used by Logstash through the NetWitness Suite user interface.

[Define a Global Audit Logging Configuration](#) provides instructions.

## Verify the Packages and Services on the Hosts

### NetWitness Suite Host

The following packages or services must be present on the NetWitness Server host:

- rsyslog-8.4.1
- rsa-audit-rt
- logstash-1.5.4-1
- rsa-audit-plugins
- rabbitmq server

### Services on a Host other than the NetWitness Suite Host

The following packages or services must be present on each of the NetWitness Suite hosts other than the NetWitness Server host:

- rsyslog-8.4.1
- rsa-audit-rt
- rabbitmq server

### Log Decoder

If you forward global audit logs to a Log Decoder, the following parser should be present and enabled:

- CEF

## Possible Issues



### What if I perform an action on a service but audit logs do not reach the configured third-party syslog server or Log Decoder?

The possible causes could be one or all of the following:

- A service is not logging to the local syslog server.
- Audit logs are not getting uploaded to RabbitMQ from the local syslog.
- Audit logs are not aggregated on the NetWitness Server host.
- Aggregated logs on the NetWitness Server host are not being forwarded to the configured third-party syslog server or Log Decoder.
- The Log Decoder is not configured to receive global audit logs in CEF format:
  - Log Decoder capture is not turned on
  - CEF Parser is not present
  - CEF Parser is not enabled

### Possible Solutions

The following table provides possible solutions for the issues.

Issue	Possible Solutions
<p>A service is not logging to the local syslog server.</p>	<ul style="list-style-type: none"> <li>• Ensure that rsyslog is up and running. You could use the following command: <code>service rsyslog status</code></li> <li>• Ensure that rsyslog is listening on port 50514 using UDP. You could use the following command: <code>netstat -tulnp grep rsyslog</code></li> <li>• Ensure the application or component is sending audit logs to port 50514. Run the tcpdump utility on the local interface for port 50514. You could use the following command: <code>sudo tcpdump -i lo -A udp and port 50514</code></li> </ul> <p>See "Solution Examples" below to view the command outputs.</p>


Issue	Possible Solutions
Audit logs are not getting uploaded to RabbitMQ from the local syslog.	<ul style="list-style-type: none"><li>• Ensure that the rsyslog plugin is up and running. You could use the following command: <pre>ps -ef grep rsa_audit_onramp</pre></li><li>• Ensure the RabbitMQ server is up and running. You could use the following command: <pre>service rabbitmq-server status</pre></li></ul> <p>See "Solution Examples" to view the command outputs.</p>
Audit logs are not aggregated on the NetWitness Server host.	<ul style="list-style-type: none"><li>• Ensure Logstash is up and running. You could use the following commands: <pre>ps -ef grep logstash service logstash status</pre></li><li>• Ensure the RabbitMQ server is up and running. You could use the following command: <pre>service rabbitmq-server status</pre></li><li>• Ensure the RabbitMQ server is listening on port 5672. You could use the following command: <pre>netstat -tulnp grep 5672</pre></li><li>• Check for any errors generated at the Logstash level. You could use the following command for the location of the log files: <pre>ls -l /var/log/logstash/logstash.*</pre></li></ul> <p>See "Solution Examples" to view the command outputs.</p>

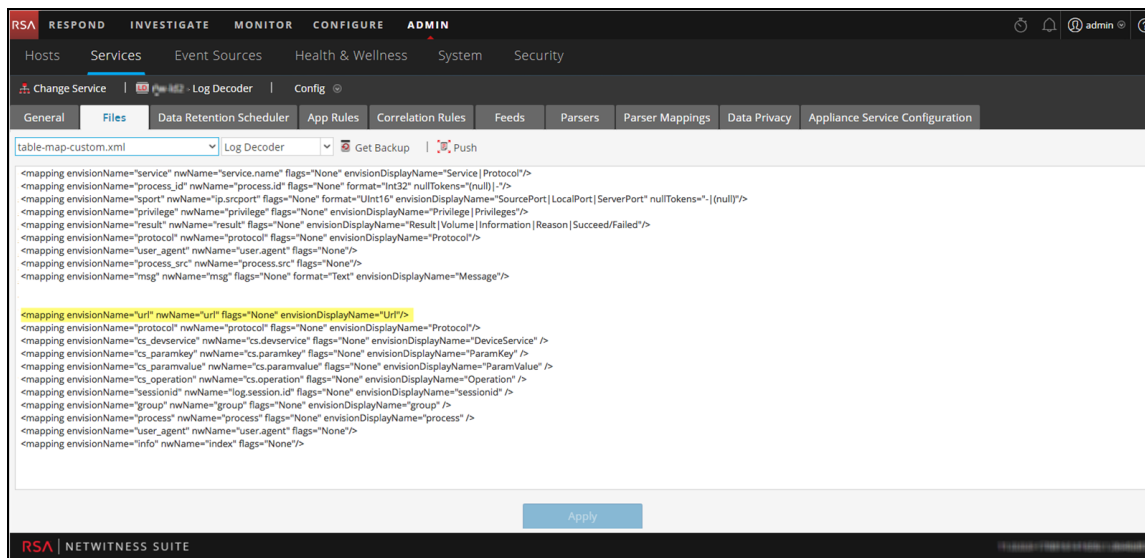
Issue	Possible Solutions
<p>Aggregated logs on the NetWitness Server host are not being forwarded to the configured third-party syslog server or Log Decoder.</p>	<ul style="list-style-type: none"><li>• Ensure Logstash is up and running. You could use the following commands: <pre>ps -ef grep logstash service logstash status</pre></li><li>• Check for any errors generated at the Logstash level. You could type the following command for the location of the log files: <pre>ls -l /var/log/logstash/logstash.</pre></li></ul> <p>See "Solution Examples" below to view the command outputs.</p> <ul style="list-style-type: none"><li>• Ensure that the destination service is up and running.</li><li>• Ensure that the destination service is listening on the correct port using the correct protocol.</li><li>• Ensure that the configured port on the destination host is not blocked.</li></ul>
<p>Audit logs forwarded from the Logstash lead to parse failure at the Log Decoder.</p>	<ul style="list-style-type: none"><li>• Ensure that you are using an appropriate notification template. Audit Logs parsed by a Log Decoder must be in CEF format. The destination from which audit logs directly or indirectly make their way to the Log Decoder must also use a CEF Template.</li><li>• The Notification Template must follow the CEF standard. Follow the steps in this guide to either use the default CEF template or create a custom CEF template following strict guidelines. <a href="#">Define a Template for Global Audit Logging</a> provides additional information.</li><li>• Verify the Logstash configuration.</li></ul>

### Why can't we see the custom metadata in Investigation?

Usually, if a meta key is not visible in Investigation, it is not being indexed. If you need to use custom meta keys for Investigations and Reporting, ensure that the meta keys that you select are indexed in the **table-map-custom.xml** file on the Log Decoder. Follow the "Maintain the Table Map Files" procedure to modify the **table-map-custom.xml** file on the Log Decoder.

Ensure that the custom meta keys are also indexed in the **index-concentrator-custom.xml** on the Concentrator. "Edit a Service Index File" provides additional information.

The following figure shows an example **table-map-custom.xml** file in NetWitness Server (ADMIN > Services > (select the Log Decoder) >  >View > Config) with a custom meta url example highlighted.




The url custom meta example is highlighted in the following code sample from the **table-map-custom.xml** file above:

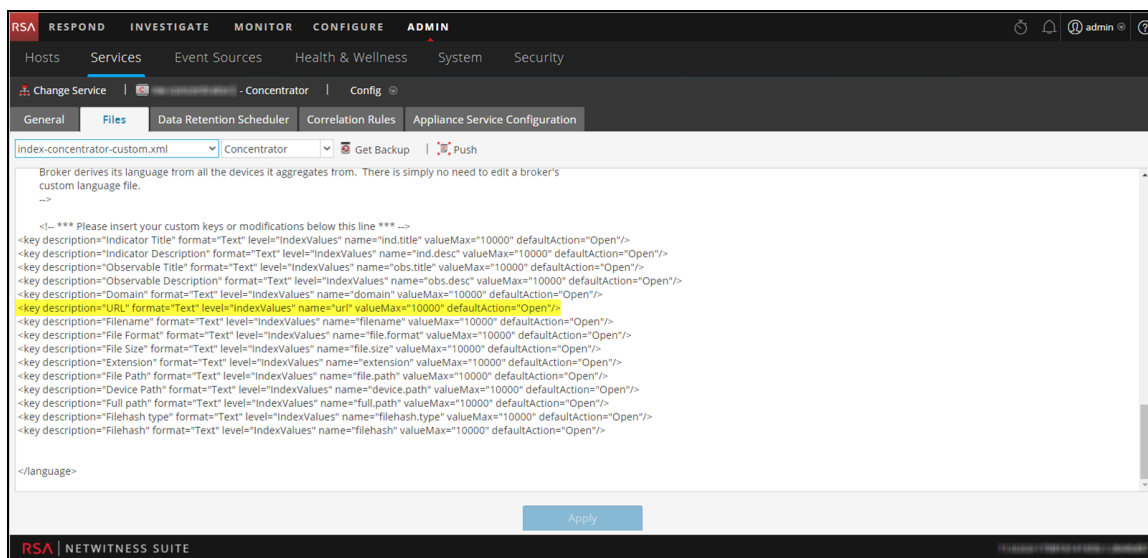
```
<mapping envisionName="url" nwName="url" flags="None"
envisionDisplayName="Url" />
<mapping envisionName="protocol" nwName="protocol" flags="None"
envisionDisplayName="Protocol" /><mapping envisionName="cs_devservice"
nwName="cs.devservice" flags="None" envisionDisplayName="DeviceService"
/><mapping envisionName="cs_paramkey" nwName="cs.paramkey" flags="None"
envisionDisplayName="ParamKey" /><mapping envisionName="cs_paramvalue"
nwName="cs.paramvalue" flags="None" envisionDisplayName="ParamValue"
/><mapping envisionName="cs_operation" nwName="cs.operation"
flags="None" envisionDisplayName="Operation" /><mapping
envisionName="sessionid" nwName="log.session.id" flags="None"
envisionDisplayName="sessionid" /><mapping envisionName="group"
```

```

nwName="group" flags="None" envisionDisplayName="group" /><mapping
envisionName="process" nwName="process" flags="None"
envisionDisplayName="process" /><mapping envisionName="user_agent"
nwName="user.agent" flags="None"/><mapping envisionName="info"
nwName="index" flags="None"/>

```

The following figure shows an example **index-concentrator-custom.xml** file in NetWitness Server (ADMIN > Services > (select the Concentrator) >  > View > Config) with a custom meta url example highlighted.



The url custom meta example is highlighted in the following code sample from the **index-concentrator-custom.xml** file above:

```

<key description="Severity" level="IndexValues" name="severity"
valueMax="10000" format="Text"/><key description="Result"
level="IndexValues" name="result" format="Text"/><key
level="IndexValues" name="ip.srcport" format="UInt16"
description="SourcePort"/><key description="Process" level="IndexValues"
name="process" format="Text"/><key description="Process ID"
level="IndexValues" name="process_id" format="Text"/><key
description="Protocol" level="IndexValues" name="protocol"
format="Text"/><key description="UserAgent" level="IndexValues"
name="user_agent" format="Text"/><key description="DestinationAddress"
level="IndexValues" name="ip.dst" format="IPv4"/><key
description="SourceProcessName" level="IndexValues" name="process.src"

```

```
format="Text"/><key description="Username" level="IndexValues"
name="username" format="Text"/><key description="Info"
level="IndexValues" name="index" format="Text"/><key
description="customdevservice" level="IndexValues" name="cs.devservice"
format="Text"/>
<key description="url" level="IndexValues" name="url" format="Text"/>
<key description="Custom Key" level="IndexValues" name="cs.paramkey"
format="Text"/><key description="Custom Value" level="IndexValues"
name="cs.paramvalue" format="Text"/><key description="Operation"
level="IndexValues" name="cs.operation" format="Text"/><key
description="CS Device Service" level="IndexValues" name="cs.device"
format="Text" valueMax="10000" defaultAction="Closed"/>
```

### Solution Examples

The following possible solution examples show the outputs of the example commands. See the above table for the complete listing of possible solutions.

#### Ensure that rsyslog is up and running

You can use the following command:

```
service rsyslog status
```

```
[root@NWAPPLIANCE22574 ~]# service rsyslog status
rsyslogd (pid 1293) is running...
[root@NWAPPLIANCE22574 ~]# █
```

#### Ensure that rsyslog is listening on port 50514 using UDP

You can use the following command:

```
netstat -tulnp|grep rsyslog
```

```
[root@NWAPPLIANCE22574 ~]# netstat -tulnp|grep rsyslog
udp        0      0 127.0.0.1:50514      0.0.0.0:*           1293/rsyslogd
[root@NWAPPLIANCE22574 ~]# █
```

#### Ensure that the application or component is sending audit logs to port 50514

The following figure shows the output of running the tcpdump utility on the local interface for port 50514.

You can use the following command:

```
sudo tcpdump -i lo -A udp and port 50514
```

```
[root@NWAPPLIANCE22574 ~]# sudo tcpdump -i lo -A udp and port 50514
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 65535 bytes
08:54:46.536420 IP NWAPPLIANCE22574.34822 > NWAPPLIANCE22574.50514: UDP, length 593
E....@.@.:.....R.Y.m<38>2015-04-24T08:54:46Z NWAPPLIANCE22574 SA_SERVER {"category":"DATA_ACCESS","deviceProduct":"Security Analytics","deviceService":"SA_SERVER","deviceVendor":"RSA","deviceVersion":"10.5.0.0","identity":"Unknown identity","operation":"/poll/oda459e3-4e9d-ca1f-20f2-8c61e31ef198","outcome":"Success","parameters":{"referrer=https://10.31.252.196/unified/dashboard/1,method=DELETE,userAgent=Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.90 Safari/537.36,queryString=token=833b67c5-6ae9-47b4-b435-560e0d38b760,remoteAddress=10.30.97.119},"severity":6}

08:54:46.615749 IP NWAPPLIANCE22574.34822 > NWAPPLIANCE22574.50514: UDP, length 365
E....@.@.:b.....R.u.<38>2015-04-24T08:54:46Z NWAPPLIANCE22574 SA_SERVER {"category":"DATA_ACCESS","deviceProduct":"Security Analytics","deviceService":"SA_SERVER","deviceVendor":"RSA","deviceVersion":"10.5.0.0","identity":"admin","key":"user.general.contextmenu","operation":"Users.preferences.,"severity":6,"userRole":"Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY"}

08:54:46.618691 IP NWAPPLIANCE22574.34822 > NWAPPLIANCE22574.50514: UDP, length 367
E....@.@.:.....R.w.<38>2015-04-24T08:54:46Z NWAPPLIANCE22574 SA_SERVER {"category":"DATA_ACCESS","deviceProduct":"Security Analytics","deviceService":"SA_SERVER","deviceVendor":"RSA","deviceVersion":"10.5.0.0","identity":"admin","key":"user.notifications.enabled","operation":"Users.preferences.,"severity":6,"userRole":"Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY"}

08:54:46.623411 IP NWAPPLIANCE22574.34822 > NWAPPLIANCE22574.50514: UDP, length 369
E....@.@.:.....R.y.<38>2015-04-24T08:54:46Z NWAPPLIANCE22574 SA_SERVER {"category":"DATA_ACCESS","deviceProduct":"Security Analytics","deviceService":"SA_SERVER","deviceVendor":"RSA","deviceVersion":"10.5.0.0","identity":"admin","key":"user.browser_timezone_zoneId","operation":"Users.preferences.,"severity":6,"userRole":"Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY"}

08:54:46.626311 IP NWAPPLIANCE22574.34822 > NWAPPLIANCE22574.50514: UDP, length 369
E....@.@.:.....R.y.<38>2015-04-24T08:54:46Z NWAPPLIANCE22574 SA_SERVER {"category":"DATA_ACCESS","deviceProduct":"Security Analytics","deviceService":"SA_SERVER","deviceVendor":"RSA","deviceVersion":"10.5.0.0","identity":"admin","key":"user.browser_timezone_zoneId","operation":"Users.preferences.,"severity":6,"userRole":"Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY"}
```

## Ensure that the rsyslog plugin is up and running

You can use the following command:

```
ps -ef|grep rsa_audit_onramp
```

```
[root@NWAPPLIANCE22574 ~]# ps -ef|grep rsa_audit_onramp
root      1636   1293   0 06:05 ?        00:00:03 /usr/sbin/rsa_audit_onramp --node_id=96b08193-a9d0-4a79-b362-87b56851f411
root      22248  6921   0 09:09 pts/0    00:00:00 grep rsa_audit_onramp
[root@NWAPPLIANCE22574 ~]#
```

## Ensure the RabbitMQ server is up and running

You can use the following command:

```
service rabbitmq-server status
```

```
[root@NWAPPLIANCE22574 ~]# service rabbitmq-server status
Status of node sa@localhost ...
[{pid,1862},
 {running_applications,
  [{rabbitmq_federation_management,"RabbitMQ Federation Management",
   "3.4.2"},
   {rabbitmq_management,"RabbitMQ Management Console","3.4.2"},
   {rabbitmq_web_dispatch,"RabbitMQ Web Dispatcher","3.4.2"},
   {webmachine,"webmachine","1.10.3-rmq3.4.2-gite9359c7"},
   {mochiweb,"MochiMedia Web Server","2.7.0-rmq3.4.2-git680dba8"},
   {rabbitmq_federation,"RabbitMQ Federation","3.4.2"},
   {rabbitmq_stomp,"Embedded Rabbit Stomp Adapter","3.4.2"},
   {rabbitmq_management_agent,"RabbitMQ Management Agent","3.4.2"},
   {rabbit,"RabbitMQ","3.4.2"},
   {ssl,"Erlang/OTP SSL application","5.3.2"},
   {public_key,"Public key infrastructure","0.21"},
   {crypto,"CRYPTO version 2","3.2"},
   {asn1,"The Erlang ASN1 compiler version 2.0.4","2.0.4"},
   {os_mon,"CPO CXC 138 46","2.2.14"},
   {inets,"INETC CXC 138 49","5.9.7"},
   {mnesia,"MNESIA CXC 138 12","4.11"},
   {amqp_client,"RabbitMQ AMQP Client","3.4.2"},
   {rabbitmq_auth_mechanism_ssl,
    "RabbitMQ SSL authentication (SASL EXTERNAL)","3.4.2"},
   {xmerl,"XML parser","1.3.5"},
   {sasl,"SASL CXC 138 11","2.3.4"},
   {stdlib,"ERTS CXC 138 10","1.19.4"},
   {kernel,"ERTS CXC 138 10","2.16.4"}]},
 {os,{unix,linux}},
 {erlang_version,
  "Erlang R16B03 (erts-5.10.4) [source] [64-bit] [smp:2:2] [async-threads:30] [kernel-poll:true]\n"},
 {memory,
```

### Ensure logstash is up and running

You can use the following commands:

```
ps -ef|grep logstash
service logstash status
```

```
[root@NWAPPLIANCE22574 ~]# ps -ef|grep logstash
logstash 1583 1 0 06:05 ? 00:01:09 /usr/bin/java -Djava.io.tmpdir=/var/lib/logstash -Xmx500m -XX:+UseParNewGC -XX:+UseConcMarkSweepGC -Djava.awt.headless=true -XX:G1InitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -jar /opt/logstash/vendor/jar/ruby-complete-1.7.11.jar -I/opt/logstash/lib /opt/logstash/lib/logstash/runner
root 8509 6921 0 09:31 pts/0 00:00:00 grep logstash
[root@NWAPPLIANCE22574 ~]# service logstash status
logstash is running
[root@NWAPPLIANCE22574 ~]#
```

### Ensure the RabbitMQ server is listening on port 5672

For example, type the following command:

```
netstat -tulnp|grep 5672
```

```
[root@NWAPPLIANCE22574 ~]# netstat -tulnp|grep 5672
tcp 0 0 127.0.0.1:5672 0.0.0.0:* LISTEN 1862/beam.smp
tcp 0 0 0.0.0.0:25672 0.0.0.0:* LISTEN 1862/beam.smp
[root@NWAPPLIANCE22574 ~]#
```

### Check for any errors generated at the Logstash level

You can type the following command for the location of the log files:

```
ls -l /var/log/logstash/logstash.*
```

```
[root@NWAPPLIANCE22574 ~]# ls -l /var/log/logstash/logstash.*
-rw-r--r--. 1 root root 0 Apr 24 06:05 /var/log/logstash/logstash.err
-rw-r--r--. 1 logstash logstash 1043 Apr 24 06:04 /var/log/logstash/logstash.log
-rw-r--r--. 1 root root 57 Apr 24 06:12 /var/log/logstash/logstash.stdout
[root@NWAPPLIANCE22574 ~]#
```

See the Possible Solutions table above for the complete listing of issues and possible solutions.



## Troubleshooting NTP Server Configuration

This topic describes NTP server configuration issues that you may encounter and suggests solutions to these problems.

### Issues Identified by Messages in the NTP Settings Panel or Log Files

This section provides troubleshooting information for issues identified by messages NetWitness Suite displays in the NTP Settings panel and log files.

	<p>User Interface: <b>Unexpected error occurred. First check the logs then contact Customer Care to resolve error.</b></p> <p><b>System Log:</b></p>
<b>Message</b>	<pre>Timestamp Level Message yyyy-dd-mmThh:mm:ss.ms ERROR com.rsa.smc.sa.adm.exception.MCOAgent Exception: No request sent, we did not discover any nodes</pre>
<b>Possible Cause</b>	Low level NetWitness Suite configuration is in error or supporting service is not running.
<b>Solution</b>	Contact Customer Care.
<b>Message</b>	User Interface: <b>Specified an invalid Hostname syntax.</b>
<b>Possible Cause</b>	Tried to enter NTP server hostname that does not confirm to IP address or FQDN syntax.
<b>Solution</b>	Reenter hostname in using correct syntax.
<b>Message</b>	User Interface: <b>Specified NTP server that already exists.</b>
<b>Possible Cause</b>	Tried to enter NTP server hostname that is already defined in NetWitness Suite.
<b>Solution</b>	Enter hostname for an NTP server not configured in NetWitness Suite.
<b>Message</b>	User Interface: <b>Cannot reach NTP server <i>hostname</i>.</b> Please verify the server address and your firewall settings.
<b>Possible Cause</b>	The server address or firewall settings may be in error.

**Solution** | Verify the server address and your firewall settings and correct them if required.

## References

---

This topic provides reference materials that describe the user interface for configuring system settings in NetWitness Suite and define parameters. Administrators use options in the Administration System view to configure system settings. Each panel is described in a separate topic.

- [Global Audit Logging Configurations Panel](#)
- [Global Notifications Panel](#)
  - [Define Notification Server Dialogs](#)
  - [Define Notification Output Dialogs](#)
  - [Define Notification Template Dialog](#)
  - [Output Tab](#)
  - [Servers Tab](#)
  - [Templates Tab](#)
- [HTTP Proxy Settings Panel](#)
- [Email Configuration Panel](#)
- [ESA Settings Panel](#)
- [Investigation Configuration Panel](#)
- [Live Services Configuration Panel](#)
- [NTP Settings Panel](#)
- [Context Menu Actions Panel](#)
- [Legacy Notifications Configuration Panel](#)

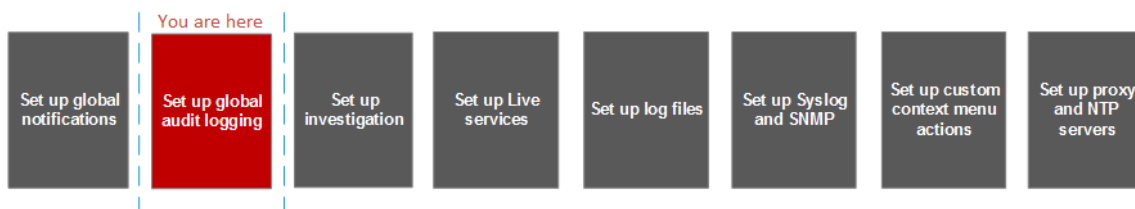
## Global Audit Logging Configurations Panel

In the **Global Audit Logging Configurations** panel (ADMIN > System > Global Auditing), you configure global audit logging by adding configurations that define how global audit logs are forwarded to external syslog systems. Global audit logs are forwarded to the selected Notification Server in your global audit logging configuration using the selected Notification Template.

Global Audit Logging provides auditors with consolidated visibility into user activities within NetWitness Suite in real-time from one centralized location.

## Workflow

This workflow shows the necessary procedures to configure and verify Global Audit Logging.



Before you can define a Global Audit Logging configuration, you need to create a Syslog Notification Server on the Global Notifications > Server tab. The Syslog Notification Server is the destination that receives the global audit logs. Next, you need to select or define an Audit Logging template on the Global Notifications > Templates tab. The Audit Logging template defines the format and message fields of the audit logs sent to the Log Decoder or third-party syslog server. If you are consuming with a Log Decoder, deploy the Common Event Format parser to your Log Decoder from Live.

**Note:** You do not need to configure the Global Notifications > Output tab for Global Audit Logging.

After you add a Global Audit Logging configuration here, audit logs are forwarded to the selected Notification Server in the configuration. Verify your audit logs to ensure that they show the audit events as defined in your audit logging template.

## What do you want to do?

Role	I want to ...	Show me how
Administrator	Create a Syslog Notification Server.	<a href="#">Configure a Destination to Receive Global Audit Logs</a>

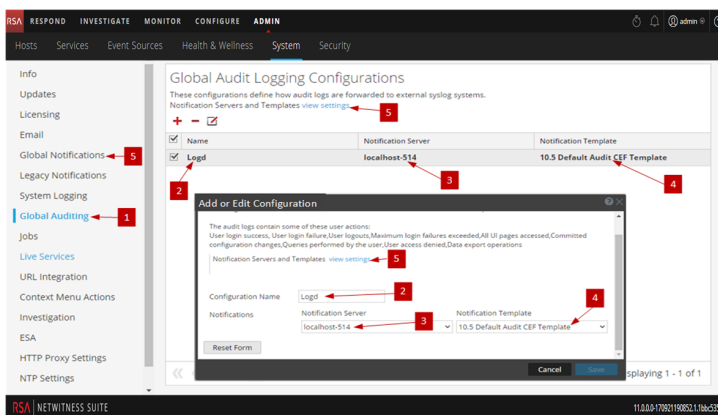
Role	I want to ...	Show me how
Administrator	Choose an Audit Logging template.	<a href="#">Define a Template for Global Audit Logging</a>
Administrator	Configure Global Audit Logging	<a href="#">Define a Global Audit Logging Configuration</a> For the complete procedure, see "Global Audit Logging - High-Level Procedure" in <a href="#">Configure Global Audit Logging</a> .
Administrator	Verify Global Audit logs	<a href="#">Verify Global Audit Logs</a>

## Related Topics

- [Troubleshoot Global Audit Logging](#)
- [Add New Configuration Dialog](#)
- [Supported CEF Meta Keys](#)
- [Supported Global Audit Logging Meta Key Variables](#)
- [Global Audit Logging Operation Reference](#)
- [Local Audit Log Locations](#)

## Quick Look

The following example illustrates a Global Audit Logging configuration. The configuration defines how NetWitness Suite forwards global audit logs to external syslog systems.






- 1 Displays the Global Audit Logging Configurations panel.
- 2 Name that identifies the Global Audit Logging configuration.

- 3 Notification Server assigned to the Global Audit Logging configuration.
- 4 Notification Template assigned to the Global Audit Logging configuration.
- 5 Displays the Global Notifications panel where you set up Servers and Templates required to configure a Global Audit Logging configuration.


## Toolbar

The following table describes the toolbar actions

Icon	Description
	Adds a global audit logging configuration.
	Deletes a global audit logging configuration. Deleting a global audit configuration does not delete the associated notification server and template. After you delete a global audit logging configuration, the forwarding of global audit logs specified in that configuration is discontinued.
	Edits a global audit logging configuration. You can change the destination of the global audit logs for your user audits by selecting a different Notification Server. You can also change the format and message fields of the global audit log entries by selecting a different Notification Template. You cannot change which NetWitness Suite user actions are logged and sent in the global audit logs.

## Configurations

The following table describes the listed configurations.

Title	Description
	To select an individual configuration, select the checkbox next to the configuration.  To select all configurations, select the checkbox in the title bar of the table.

Title	Description
Name	Displays the name of the global auditing configuration. For example, you can name the configurations based on the destination of the global audit logs, such as HQ SA and My Syslog Server.
Notification Server	Displays the Syslog Notification Server selected as the destination for the global audit logs. If you want to forward global audit logs to a Log Decoder, create a Syslog type of Notification Server. <a href="#">Configure a Destination to Receive Global Audit Logs</a> provides instructions on how to create a Syslog Notification Server for global audit logging.
Notification Template	<p>Displays the Audit Logging Notification Template selected for the configuration. It defines the format and message fields of the audit log entries.</p> <p>For Log Decoders, use the <b>Default Audit CEF Template</b>. You can add or remove fields from the Common Event Format (CEF) template if you have specific requirements. <a href="#">Define a Template for Global Audit Logging</a> provides instructions and <a href="#">Supported CEF Meta Keys</a> describes the available CEF meta keys.</p> <p>For, third-party syslog servers, you can use a default audit logging template or define your own format (CEF or non-CEF). <a href="#">Define a Template for Global Audit Logging</a> provides instructions and <a href="#">Supported Global Audit Logging Meta Key Variables</a> describes the available meta key variables.</p>

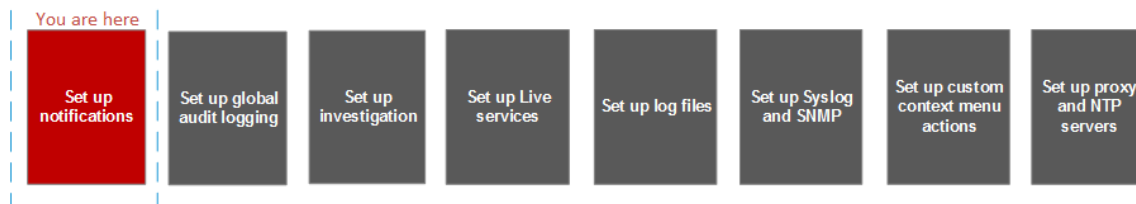
## Global Notifications Panel

Global Notifications panel introduces the features for configuring notification settings. Global Notifications configurations define notifications settings for Event Source Management (ESM), Health and Wellness, Global Audit Logging, Event Stream Analysis (ESA), and Respond.

In the Global Notifications panel, you can configure the following global notification settings:

- Notification Outputs
- Notification Servers
- Templates

## WorkFlow



## What do you want to do?

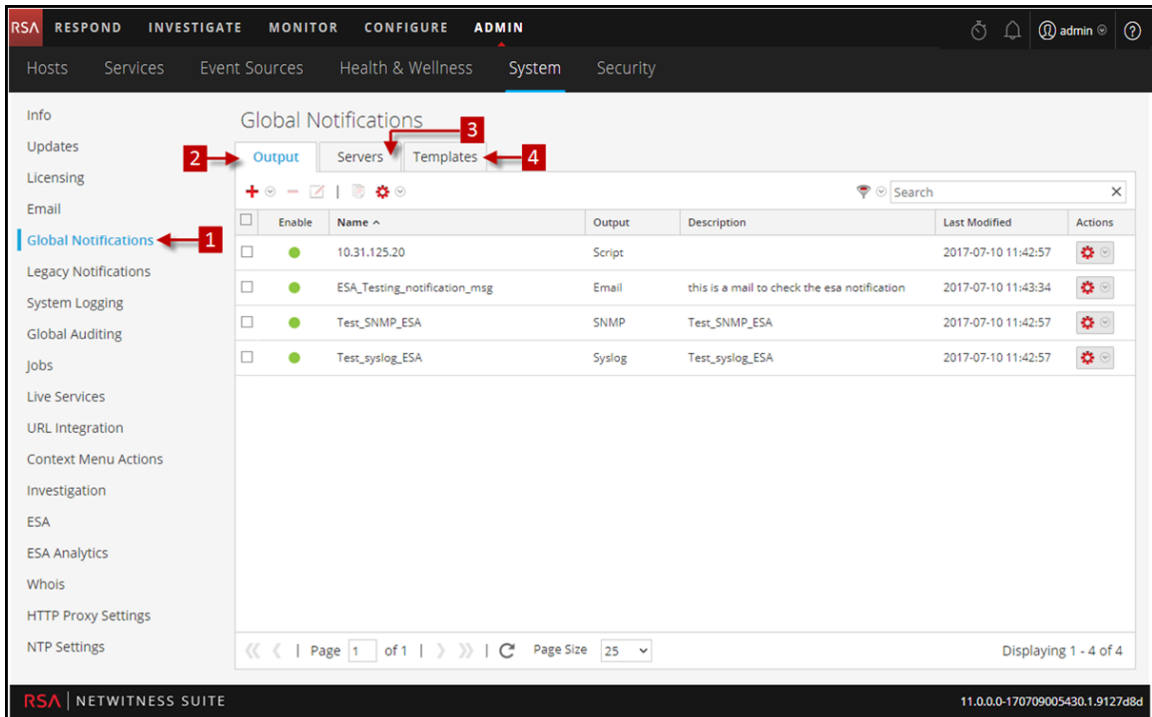
Role	I want to ...	Show me how
Administrator	Configure Notification Servers	<a href="#">Servers Tab</a>
Administrator	Configure Notification Outputs	<a href="#">Output Tab</a>
Administrator	Configure Notification Templates	<a href="#">Templates Tab</a>

## Related Topics

- [Configure a Syslog Notification Server](#)
- [Configure Script as a Notification Server](#)

## Quick Look








- 1 Displays the Global Notification Panel.
- 2 Displays the Output Tab
- 3 Displays the Servers Tab
- 4 Displays the Templates Tab

## Toolbar and Features




The Global Notifications panel has three tabs: Output, Servers, and Templates.

Feature	Description
<b>Output tab</b>	This tab enables you to configure notification outputs. See Output Tab for more information.
<b>Servers tab</b>	This tab enables you to configure notification servers. See Servers Tab for more information.
<b>Templates tab</b>	This tab enables you to configure notification templates. See Templates Tab for more information.

This table describes the columns in the grid for Notification Outputs and Notification Servers.

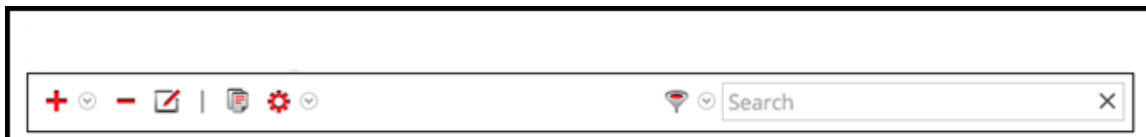
Column	Description
	Selects a row for an action in the toolbar. Clicking the checkbox in the column title selects or deselects all rows in the grid.
<b>Enable</b>	Indicates whether the configuration is enabled. A solid colored green circle indicates that a configuration is enabled. A blank white circle indicates that a configuration is not enabled.
<b>Name</b>	A name that identifies or labels the configuration.
<b>Output</b>	The configuration output. The outputs are Email, SNMP, Syslog, and Script.
<b>Description</b>	A brief description about the configuration.
<b>Last Modified</b>	Shows the date and time of the last configuration change.
<b>Actions</b>	Provides an Actions menu   for the selected configuration with actions that can be taken on the configuration. The Actions menu enables you to delete, edit, duplicate, and export the configuration.

This table describes the columns in the grid for Notification Templates.

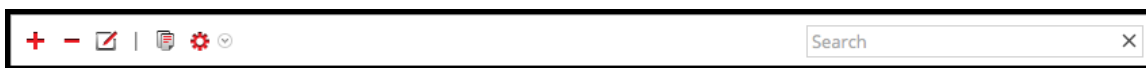
Column	Description
	Selects a row for an action in the toolbar. Clicking the checkbox in the column title selects or deselects all rows in the grid.
<b>Name</b>	A name that identifies or labels the template.
<b>Template Type</b>	The type of template. The types are Audit Logging, Event Stream Analysis, Event Source Monitoring, and Health Alarms.
<b>Description</b>	A brief description about the template.
<b>Actions</b>	Provides an Actions menu   for the selected configuration with actions that can be taken on the template. The Actions menu enables you to delete, edit, duplicate, and export the template.

## Global Notifications Panel Toolbar


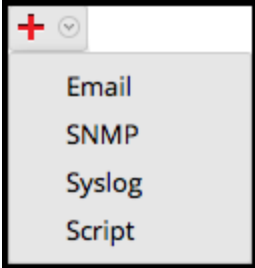






The Global Notifications panel toolbar is at the top of the Output, Servers, and Templates tabs. The following figure shows the toolbar on the Output and Servers tabs.



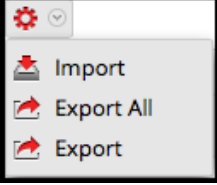

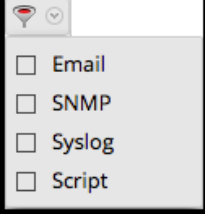



The following figure shows the toolbar on the Templates tab.



The following table describes the features of the Global Notifications panel toolbar.

Feature	Description
  	<p>Adds a notification server on the Servers tab, adds a notification output (notification) on the Output tab, and adds a notification template on the Templates tab.</p> <p>On the Servers and Output tabs, you can select to configure Email, SNMP, Syslog, and Script notification settings.</p>
	<p>Removes a selected notification configuration.</p> <p>You cannot delete notification servers and notification types that are associated with global audit log configurations.</p> <p>If you attempt to delete a notification output (notification) being used by alerts, you will receive a warning confirmation message that the alerts using the notification will not function properly. The message shows the number of alerts in use.</p> <p>You can also delete a configuration by selecting a configuration and then in the Actions column, selecting   &gt; Delete.</p>
	<p>Edits a selected notification configuration. You can also edit a configuration by selecting a configuration and then in the Actions column, selecting   &gt; Edit.</p>

Feature	Description
	<p>Duplicates a selected notification configuration. You can also duplicate a configuration by selecting a configuration and then in the Actions column, selecting  &gt; Duplicate.</p>
	<p>Displays the following options:</p> <ul style="list-style-type: none"> <li>• <b>Import:</b> Imports a notification server, type, or template. For example, on the Servers tab, you can import a notification server configuration.</li> <li>• <b>Export All:</b> Exports all of the configurations. For example, if you are on the Servers tab, you can export all of the notification server configurations.</li> <li>• <b>Export:</b> Exports a selected configuration. You can also export a configuration by selecting a configuration and then in the Actions column, selecting  &gt; Export.</li> </ul>
	<p>Filters by Email, SNMP, Syslog, or Script.</p>
	<p>Searches configurations in the grid.</p>

## Define Notification Server Dialogs

This topic describes the Define Notification Server dialogs used to configure the settings of the various types of notification servers. You configure notification servers in the Administration > System > Notifications > Servers tab.

Notifications are used by a variety of components in NetWitness Suite, such as Event Stream Analysis (ESA), RESPOND, and Global Audit Logging. Notification settings are called Notification Servers. In the Servers tab of the Administration System view Notifications panel, you can create multiple Notification Server configurations.

You can configure the following types of notification server settings in NetWitness Suite:

- Email
- SNMP
- Syslog
- Script

For Global Audit Logging, you can only use Syslog Notification Servers.

Procedures related to notification servers are described in [Configure Notification Servers](#).

To access the Define Notification Server dialogs:

1. Go to **ADMIN > System**.
2. In the left navigation panel, select **Global Notifications**.
3. In the **Notifications Servers** panel, click **+** and then select a type of notification server (Email, SNMP, Syslog, or Script)

The Define Notification Server dialog is displayed for your selection.

There are four notification server dialogs, which allow you to configure notification servers.

### Email

Email notification servers enable you to configure email server settings to send alert notifications.

The following figure shows the Define Email Notification Server dialog.

The screenshot shows a dialog box titled "Define Email Notification Server". It contains the following fields and controls:

- Enable:** A checked checkbox.
- Name \*:** A text box containing "Outbound SMTP via GMAIL".
- Description:** A text box containing "This server uses Google mail to send alerts outside".
- Server IP Or Hostname \*:** A text box containing "smtp.google.com".
- Server Port:** A text box containing "25".
- SSL:** A checked checkbox.
- From Email Address \*:** A text box containing "esa@gmail.com".
- Username:** A text box containing "esa".
- Password:** A text box containing "..." (masked).
- Max Alerts Per Minute:** A text box containing "500".
- Max Alert Wait Queue Size:** A text box containing "100" followed by a question mark.

At the bottom right, there are two buttons: "Cancel" and "Save".

The following table lists the various parameters that you need to define for the email notification servers.

Parameters	Description
Enable	Select to enable the notification server.
Name	A name to identify or label the notification server.
Description	A brief description about the notification server.
Server IP Or Hostname	Hostname of the email server. For ESM/SMS and ESA notifications, you must specify only the hostname/FQDN.
Server Port	The server port.
SSL	Select the option if you want the communication to happen through SSL.

Parameters	Description
From EMail Address	Email account from which you want to send email notifications.
Username	Username for logging into the email account if the SMTP server requires user authentication to relay emails successfully.
Password	User password for logging into the email account if the SMTP server requires user authentication to relay emails successfully.
Max Alerts Per Minute	Describes the maximum number of alerts per minute.
Max Alert Wait Queue Size	Describes the maximum number of alerts to be queued before they are dropped.

### **SNMP**

SNMP notification servers enable you to configure SNMP trap host settings as a notification server to send alert notifications.

The following figure shows the Define SNMP Notification Server dialog.

### Define SNMP Notification Server ? X

The Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. SA can send audit event as SNMP traps to a configured SNMP trap host.

Enable	<input checked="" type="checkbox"/>
Name*	<input type="text" value="SNMP Trap Receiver"/>
Description	<input type="text" value="This is the SNMPv3 trap receiver in the deployment"/>
Server IP Or Hostname*	<input type="text" value="localhost"/>
Server Port	<input type="text" value="162"/>
SNMP Version	<input type="text" value="V3"/>
Security Name	<input type="text" value="esa"/>
Security Level	<input type="text" value="Authenticated and Unencrypted"/>
Auth Protocol	<input type="text" value="Unauthenticated and Unencrypted"/>
Auth Key	<input type="text" value="Authenticated and Unencrypted"/>
Number Of Retries	<input type="text" value="1"/>
Max Alerts Per Minute	<input type="text" value="1000"/>
Max Alert Wait Queue Size:	<input type="text" value="0"/> ?

The following table lists the various parameters that you need to define for the SNMP notification servers.

Parameter	Description
Enable	Select to enable the notification server.
Name	A name to identify or label the notification server.
Description	A brief description about the notification server.
Server IP Or Hostname	SNMP trap host IP address or hostname.



Parameter s	Description
Server Port	Listening port number on the SNMP trap host.

Parameters	Description								
SNMP Version	<p>SNMP version. The following are the options:</p> <ul style="list-style-type: none"> <li>• V1</li> <li>• V2C</li> <li>• V3</li> </ul> <p>If you select SNMP Version 3 (v3), the following parameters are displayed:</p> <table border="1" data-bbox="402 688 1182 1780"> <thead> <tr> <th data-bbox="402 688 699 743">Parameters</th> <th data-bbox="699 688 1182 743">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="402 743 699 1297">Notification Type</td> <td data-bbox="699 743 1182 1297"> <p>Based on the notification type a SNMP messages are sent each time an alert is generated.</p> <p>The following notification types are supported:</p> <ul style="list-style-type: none"> <li>• Inform - Inform is acknowledged trap. The sender gets an acknowledgement from the receiver.</li> <li>• Trap - Trap is unacknowledged notification</li> </ul> </td> </tr> <tr> <td data-bbox="402 1297 699 1507">Authoritative Engine ID (This option is available only for notification type TRAP)</td> <td data-bbox="699 1297 1182 1507"> <p>An identifier which is used to identify the agents. Authoritative engine ID along with the username is used to uniquely identify the agent.</p> </td> </tr> <tr> <td data-bbox="402 1507 699 1780">Security Level</td> <td data-bbox="699 1507 1182 1780"> <p>Define the security level. The following are the options:</p> <ul style="list-style-type: none"> <li>• Unauthenticated and Unencrypted</li> <li>• Authenticated and Unencrypted</li> <li>• Authenticated and Encrypted</li> </ul> </td> </tr> </tbody> </table>	Parameters	Description	Notification Type	<p>Based on the notification type a SNMP messages are sent each time an alert is generated.</p> <p>The following notification types are supported:</p> <ul style="list-style-type: none"> <li>• Inform - Inform is acknowledged trap. The sender gets an acknowledgement from the receiver.</li> <li>• Trap - Trap is unacknowledged notification</li> </ul>	Authoritative Engine ID (This option is available only for notification type TRAP)	<p>An identifier which is used to identify the agents. Authoritative engine ID along with the username is used to uniquely identify the agent.</p>	Security Level	<p>Define the security level. The following are the options:</p> <ul style="list-style-type: none"> <li>• Unauthenticated and Unencrypted</li> <li>• Authenticated and Unencrypted</li> <li>• Authenticated and Encrypted</li> </ul>
Parameters	Description								
Notification Type	<p>Based on the notification type a SNMP messages are sent each time an alert is generated.</p> <p>The following notification types are supported:</p> <ul style="list-style-type: none"> <li>• Inform - Inform is acknowledged trap. The sender gets an acknowledgement from the receiver.</li> <li>• Trap - Trap is unacknowledged notification</li> </ul>								
Authoritative Engine ID (This option is available only for notification type TRAP)	<p>An identifier which is used to identify the agents. Authoritative engine ID along with the username is used to uniquely identify the agent.</p>								
Security Level	<p>Define the security level. The following are the options:</p> <ul style="list-style-type: none"> <li>• Unauthenticated and Unencrypted</li> <li>• Authenticated and Unencrypted</li> <li>• Authenticated and Encrypted</li> </ul>								

Parameters	Description	
	Auth Protocol ( This option is available only for security level Authenticated and Unencrypted and Authenticated and Encrypted)	Authentication protocol which is used to validate a user before providing an access to the server. The options are: <ul style="list-style-type: none"> <li>• SHA</li> <li>• MD5</li> </ul>
	Auth Key ( This option is available only for security level Authenticated and Unencrypted and Authenticated and Encrypted)	A password that you want to use for authentication.
	Privacy Protocol ( This option is available only for security level Authenticated and Encrypted)	Privacy protocol is an encryption technique for data communication.
	Private Key ( This option is available only for security level Authenticated and Encrypted)	A password that you want to use for encryption.
Community	Community string used to authenticate on the SNMP trap host. The default value is <b>public</b> .	

Parameter s	Description
Number of Retries	Number of retries for the trap.
Max Alerts Per Minute	Maximum number of alerts per minute.
Max Alert Wait Queue Size	Maximum number of alerts to be queued before they are dropped.

### Syslog

Syslog notification servers allow you to configure Syslog settings as a notification server to send notifications. When enabled, Syslog provides auditing through the use of the RFC 5424 Syslog protocol. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis.

You cannot disable notification servers associated with global audit logging configurations.

The following figure shows the Define Syslog Notification Server dialog.

### Define Syslog Notification Server ✕

Provides auditing through the use of the RFC 5424 syslog protocol. Regulations, such as SOX, PCI DSS, HIPAA, and many others are requiring organizations to implement comprehensive security measures, which often include collecting and analyzing logs from many different sources. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis.

Enable

Name\*

Description

Server IP Or Hostname\*

Server Port

Protocol

Facility

Max Alerts Per Minute

Max Alert Wait Queue Size:  ?

The following table lists the various parameters that you need to define for the Syslog notification servers.

Parameters	Description
Enable	Select to enable the notification server.
Name	A name to identify or label the notification server.
Description	A brief description about the notification server.
Server IP Or Hostname	The hostname of the host where the target Syslog process is running.
Server Port	The port number where the target Syslog process is listening.
Protocol	The protocol to be used to transfer the Syslog files.

Parameters	Description
Facility	<p>The designated Syslog facility to use for all outgoing messages.</p> <p>It is used to specify what type of program is logging the message. Some possible values are KERN, USER, MAIL, and DAEMON. This lets the configuration file specify that messages from different facilities will be handled differently.</p>
Max Alerts Per Minute	<p>Maximum number of alerts per minute.</p> <p>This field is not used for Global Audit Logging.</p>
Max Alert Wait Queue Size	<p>Maximum number of alerts to be queued before they are dropped.</p> <p>This field is not used for Global Audit Logging.</p>

## Script

Script notification servers enable you to configure Script as a Notification Server.

The following figure shows the Define Script Notification Server dialog.

The following table lists the various parameters that you need to define for the Script notification servers.

Parameters	Description
Enable	Select to enable the notification server.

Parameters	Description
Name	A name to identify or label the notification server.
Description	A brief description about the notification server.
Run As User	Name of the user identity under which the script is executed. The default user identity is <b>notification</b> . For ESA, you cannot set this to anything else unless you have created the account on the ESA host.
Max Runtime (Sec)	The maximum time (in seconds) the script is allowed to run.

## Define Notification Output Dialogs

This topic provides descriptions of the various notification output dialogs. You configure notification outputs in the ADMIN > System > Notifications > Output tab. Notifications are basically the destinations used for sending notifications. For ESA, notifications enable you to define how you want to receive the ESA alerts. The following are the different notifications supported by NetWitness Suite:

- Email
- SNMP
- Syslog
- Script

Procedures related to notifications are described in [Configure Notification Outputs](#).

To access the Define Notification dialogs:

1. Go to **ADMIN > System**.
2. In the options panel, select **Global Notifications**.
3. On the **Output** tab, click **+** and then select a notification output (Email, SNMP, Syslog, or Script)

The Define Notification dialog is displayed for your selection.

There are four notification dialogs, which allow you to configure notification outputs.

### Email

Email notifications enable you to define the destination email address to which you can send the alerts. It also enables you to add a custom description in the subject of the email and also to define multiple destination email addresses.

The following figure shows the Define Email Notification dialog.



The following table lists the various parameters that you need to define for the email notifications.

Parameter	Description
Enable	Select to enable the notification.
Name	A name to identify or label the notification.
Description	A brief description about the notification.
To Email Addresses	Describes the destination email address to which the alert needs to be sent. <b>Note:</b> You can define multiple email addresses.
Subject Template Type	Lists available templates for creating a subject. When you choose a template, the Subject field is automatically filled in with the code for your chosen template.
Subject	Custom description about the triggered alert. This information is automatically filled in if you choose one of the predefined templates from the Subject Template Type drop-down menu. <b>Note:</b> To provide a custom subject, please refer to "Include the Default Email Subject Line" topic in the <i>System Maintenance Guide</i> .

## SNMP

SNMP notifications enable you to define the SNMP settings to send alert notifications.

The following figure shows the Define SNMP Notification dialog.

The Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. SA can send audit event as SNMP traps to a configured SNMP trap host.

Enable

Name \*

Description

Trap OID

Message OID

Variables + -

<input checked="" type="checkbox"/>	Name	Value
<input checked="" type="checkbox"/>	1.3.6.1.2.1.25	Security Analytics

Cancel Save

The following table lists the various parameters that you need to define for the SNMP notifications.

Parameter	Description
Enable	Select to enable the notification.
Name	A name to identify or label the notification.
Description	A brief description about the notification.
Trap OID	The object ID for the SNMP trap on the trap host that receives the event. The default value is <b>1.3.6.1.4.1.36807.1.20.1</b> . This value is a hierarchical name that represents the system that generates the trap. 1.3.6.1.4.1 is the common prefix for all enterprises and 36807.1.20.1 identifies NetWitness Suite.

Parameter	Description
Message OID	The message object identifier for the SNMP trap.
Variables	Additional information that should be included within the trap. It is a variable that is a name value pair.

## Syslog

Syslog notifications enable you to define the Syslog settings to send alert notifications.

The following figure shows the Define Syslog Notification dialog.

**Define Syslog Notification**

Provides auditing through the use of the RFC 5424 syslog protocol. Regulations, such as SOX, PCI DSS, HIPAA, and many others are requiring organizations to implement comprehensive security measures, which often include collecting and analyzing logs from many different sources. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis.

Enable

Name \*

Description

Severity

Encoding

Max Length

Include Local Timestamp

Include Local Hostname

Identity String

Cancel Save

The following table lists the various parameters that you need to define for the Syslog notifications.

Parameter	Description
Enable	Select to enable the notification.

Parameter	Description
Name	A name to identify or label the notification.
Description	A brief description about the notification.
Severity	Defines the severity of the alert.
Encoding	Defines the encoding format. In some environments where no regular character sets are used (for example, Japanese characters), this field will help selecting the right encoding of the characters.
Max Length	The maximum length of a Syslog message in bytes. The default value is <b>2048</b> .  Messages that exceed the maximum length are truncated when the <b>Truncate overly large syslog messages</b> checkbox is selected, which is found in Administration > System > Legacy Notifications. <a href="#">Legacy Notifications Configuration Panel</a> provides additional information.
Include Local Timestamp	Select to include the local timestamp in messages.
Include Local Hostname	Select to include the local hostname in Syslog messages.
Identity String	An identity string to be prefixed to each Syslog alert. If the string is blank, no identity string is prefixed to the outgoing Syslog alerts. You can use this to identify the alerts from ESA.

## Script

Script notifications enable you to define the Script that executes in response to the alert. You can use any script for ESA notifications.

The following figure shows the Define Script Notification dialog.

Define Script Notification
?

Enable

Name \*

Description

Script \* 1

```
#!/usr/bin/env python
import json
import sys
def invoke_rest_API(alert):
    """
    Alert details are available in the Python hash passed to this method
    e.g. alert['id'], alert['severity'], alert['module_name'], alert['events'][0],
    etc. These can be used to implement the external integration required.
    """
    pass

# The default SCRIPT template passes the entire alert rendered as a JSON string
if __name__=="__main__":
    invoke_rest_api(json.loads(sys.argv[1]))
sys.exit(0)
```

Cancel
Save

The following table lists the various parameters that you need to define for the Script notifications.

Parameter	Description
Enable	Select to enable the notification.
Name	A name to identify or label the notification.
Description	A brief description about the notification.
Script	Defines the script.

## Define Notification Template Dialog


In the Global Notifications panel, you can configure global notification settings for Notification Servers, Notification Outputs, and Notification Templates. On the Templates tab, you configure the templates for various notifications. The notification template defines the format and message fields of the notifications. You can select a default template or you can use the Define Template dialog to configure and edit templates.

You can define the following template types:

- Audit Logging
- Event Stream Analysis
- Event Source Monitoring
- Health Alarms

Procedures related to notification templates are described in [Configure Templates for Notifications](#).

To access the Define Template dialog:

1. Go to **ADMIN > System**.
2. In the left navigation panel, select **Global Notifications > Template Tab**.
3. In the **Notifications Configurations** panel, click **+**, or select a configuration and click .

The **Define Template** dialog is displayed.

## Features

The following table describes the features in the Define Template dialog.

Field	Description
Name	Type a unique name for the notification template.
Template Type	Select the type of template that you want to create: <ul style="list-style-type: none"> <li>• <b>Audit Logging:</b> Use this template for Global Audit Logging.</li> <li>• <b>Event Stream Analysis:</b> Use this template type for ESA alert notifications.</li> <li>• <b>Event Source Monitoring:</b> Use this template type for ESM notifications.</li> <li>• <b>Health Alarms:</b> Use this template type for Health and Wellness notifications.</li> </ul>

Field	Description
Description	Add a description for the template. For example, if you create a notification template for Log Decoders to use for Global Audit Logging, you could mention that information in the description.
Template	Specify the format for the template. <a href="#">Define a Template for Global Audit Logging</a> provides instructions on how to define an audit logging template to use for Global Audit Logging. To define a template for Event Stream Analysis (ESA), see <a href="#">Define a Template for ESA Alert Notifications</a> .



## Output Tab

In the **Global Notifications** panel, in the **Output** tab (Admin > System > Notifications > Output), you configure notification outputs. Global Notifications configurations define notifications settings for Event Source Management (ESM), Health and Wellness, Global Audit Logging, Event Stream Analysis (ESA), and RESPOND.

**Notification Output** configurations define email addresses and subject lines, SNMP trap OID settings, syslog output settings, and script code.

Notifications are the destinations configured for the alert notifications that are sent by ESA service. You can configure the following as destinations using the Output tab:

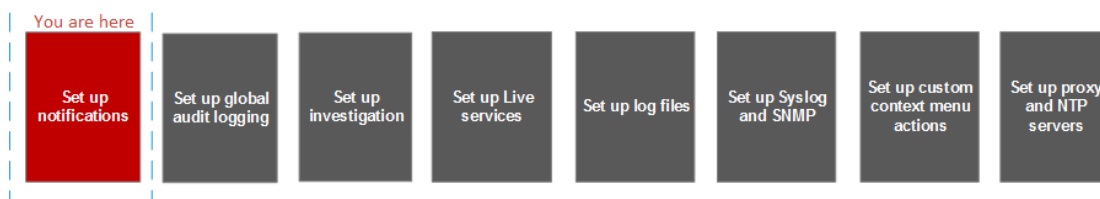
- Email
- SNMP
- Syslog
- Script

**Note:** You do not need to configure the Output tab for Global Audit Logging. For detailed steps, see [Configure Global Audit Logging](#).

### Workflow

This workflow shows the necessary procedures to configure and verify the output for Global Notifications. You can perform the following:

- Configure the Email settings as notification.
- Configure SNMP settings as notification.
- Configure Syslog settings as notification.
- Configure a Script as notification.



### What do you want to do?

Role	I want to ...	Show me how
Administrator	Define notification outputs.	<a href="#">Configure Notification Outputs</a>

## Related Topics

- [Notification Outputs Overview](#)
- [Configure Email as a Notification](#)
- [Configure Script as a Notification](#)
- [Configure SNMP as a Notification](#)
- [Configure Syslog as a Notification](#)


## Quick Look

The following example illustrates Global Notification Outputs configuration.

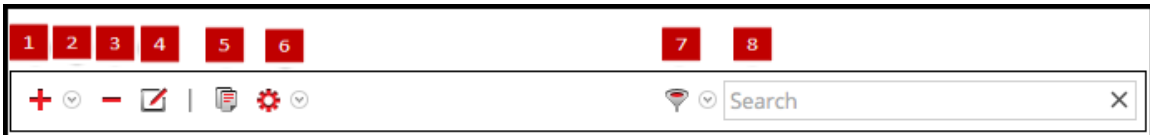
The screenshot displays the 'Global Notifications' configuration page in the RSA NetWitness Suite. The page features a table with the following columns: Enable, Name, Output, Description, Last Modified, and Actions. The table contains five rows of notification configurations. Red callout boxes are placed over the interface to highlight specific features: 1 points to the toolbar, 2 points to the 'Enable' column, 3 points to the 'Name' column, 4 points to the 'Output' column, 5 points to the 'Description' column, 6 points to the search bar, and 7 points to the 'Actions' column.





1	2	3	4	5	6	7
Enable	Name	Output	Description	Last Modified	Search	Actions
<input type="checkbox"/>	10.31.125.20	Script		2017-07-10 19:42:57		
<input type="checkbox"/>	ESA_Testing_notification_msg	Email	this is a mail to check the esa notification	2017-07-10 19:43:34		
<input type="checkbox"/>	Test_SNMP_ESA	SNMP	Test_SNMP_ESA	2017-07-10 19:42:57		
<input type="checkbox"/>	Test_syslog_ESA	Syslog	Test_syslog_ESA	2017-07-10 19:42:57		
<input type="checkbox"/>	snmp v3	SNMP		2017-07-11 14:59:30		

- 1 Selects a row for an action in the toolbar. Selecting the check box in the column title selects or deselects all rows in the grid.
- 2 Indicates whether the configuration is enabled. A solid colored green circle indicates that a configuration is enabled. A blank white circle indicates that a configuration is not enabled.
- 3 Identifies or labels the configuration.
- 4 Identifies the configuration output. The outputs are Email, SNMP, Syslog, and Script.
- 5 Describes the configuration.

- 6 Shows the date and time of the last configuration change.
- 7 Provides an Actions menu  for the selected configuration with actions that can be taken on the configuration. The Actions menu enables you to delete, edit, duplicate, and export the configuration.

The Global Notifications panel toolbar is at the top of the Output tag and provides the following options:



- 1 Adds a notification output
- 2 Configures Email, SNMP, Syslog, and Script notification settings.
- 3 Removes a selected notification configuration. You cannot delete notification servers and notification types that are associated with global audit log configurations. If you attempt to delete a notification output (notification) being used by alerts, you will receive a warning confirmation message that the alerts using the notification will not function properly. The message shows the number of alerts in use. You can also delete a configuration by selecting a configuration and then in the Actions column, selecting  > Delete.
- 4 Edits a selected notification configuration. You can also edit a configuration by selecting a configuration and then in the Actions column, selecting  > Edit.
- 5 Duplicates a selected notification configuration. You can also duplicate a configuration by selecting a configuration and then in the Actions column, selecting  > Duplicate.
- 6 Displays the following options:
  - **Import:** Imports a notification server, type, or template. For example, on the Servers tab, you can import a notification server configuration.
  - **Export All:** Exports all of the configurations. For example, if you are on the Servers tab, you can export all of the notification server configurations.
  - **Export:** Exports a selected configuration. You can also export a configuration by selecting a configuration and then in the Actions column, selecting  > Export.
- 7 Filters by Email, SNMP, Syslog, or Script.
- 8 Searches configurations in the grid.

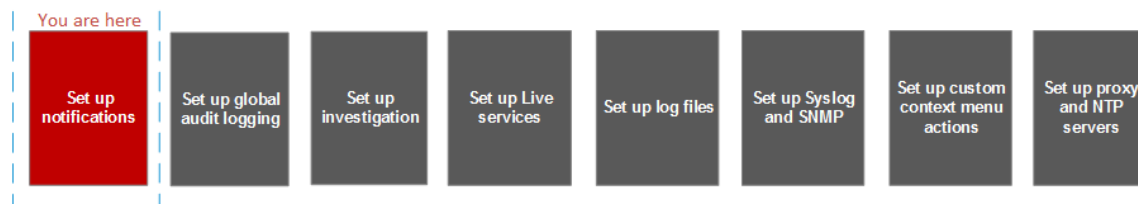
## Servers Tab

Servers Tab describes the components of the Global Notifications > Servers tab. This tab enables to configure notification servers. Global Notifications configurations define notifications settings for Event Source Management (ESM), Health and Wellness, Global Audit Logging, Event Stream Analysis (ESA), and RESPOND.

Configure **Notification Servers** in the Servers tab. On the Servers tab, add the servers from which you want to receive notifications from the system. For Global Audit Logging, define Log Decoders as Syslog Notification Servers.

Event Stream Analysis can send notifications to users through email, SNMP, or Syslog when an alert is triggered on the ESA service. These alert notification senders are called Notification Servers. You can configure multiple notification settings and use them while defining an ESA rule, for example, you can configure multiple mail servers or Syslog servers and use the settings while defining an ESA rule.

### Workflow



The workflow shows the necessary procedures to configure and verify the Servers for Global Notifications. You can perform the following:

- Configure the Email settings as a notification server.
- Configure SNMP settings as a notification server.
- Configure Syslog settings as a notification server.
- Configure a Script as a notification server.

### What do you want to do?

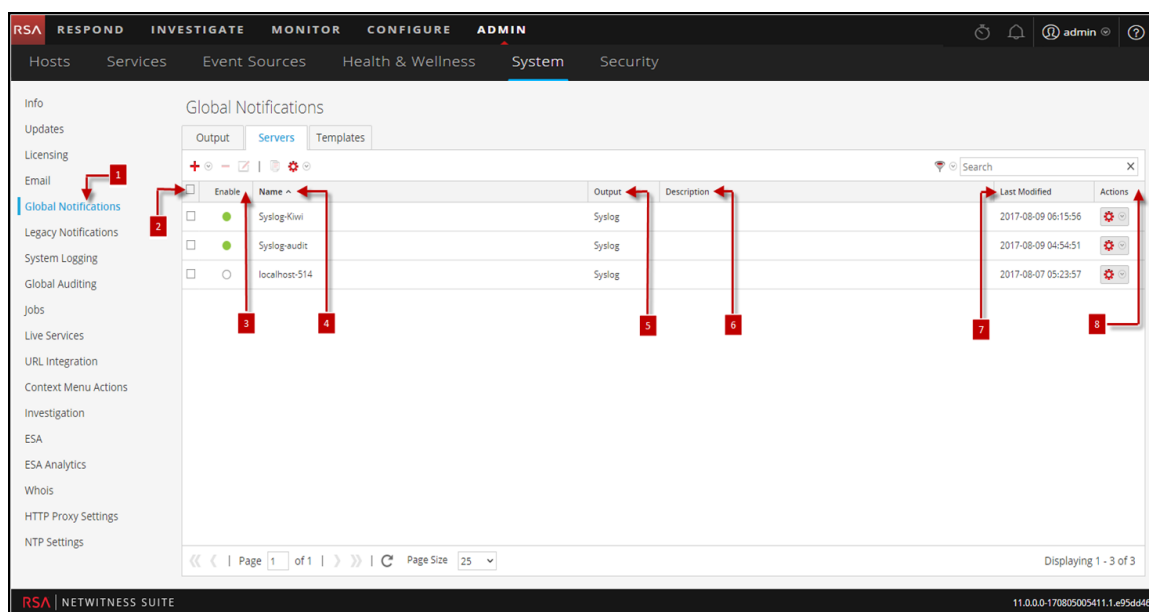
Role	I want to ...	Show me how
Administrator	Define notification Servers	<a href="#">Configure Notification Servers</a>


## Related Topics

- [Notification Servers Overview](#)
- [Configure the Email Settings as Notification Server](#)
- [Configure Script as a Notification Server](#)
- [Configure the SNMP Settings as Notification Server](#)
- [Configure a Syslog Notification Server](#)

## Quick Look

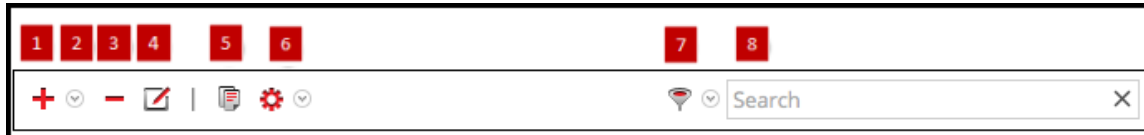
The following example illustrates Global Notification Servers configuration.







- 1 Displays the Server Tab Panel.
- 2 Selects a row for an action in the toolbar. Selecting the checkbox in the column title selects or deselects all rows in the grid.
- 3 Indicates whether the configuration is enabled. A solid colored green circle indicates that a configuration is enabled. A blank white circle indicates that a configuration is not enabled.
- 4 Identifies or labels the configuration.
- 5 Identifies the configuration output. The outputs are Email, SNMP, Syslog, and Script.
- 6 Describes the configuration.
- 7 Shows the date and time of the last configuration change.
- 8 Provides an Actions menu  for the selected configuration with actions that can be

taken on the configuration. The Actions menu enables you to delete, edit, duplicate, and export the configuration.

The Global Notifications panel toolbar is at the top of the Output tag and provides the following options:



- 1 Adds a notification output
- 2 Configures Email, SNMP, Syslog, and Script notification settings.
- 3 Removes a selected notification configuration. You cannot delete notification servers and notification types that are associated with global audit log configurations. If you attempt to delete a notification output (notification) being used by alerts, you will receive a warning confirmation message that the alerts using the notification will not function properly. The message shows the number of alerts in use. You can also delete a configuration by selecting a configuration and then in the Actions column, selecting  > Delete.
- 4 Edits a selected notification configuration. You can also edit a configuration by selecting a configuration and then in the Actions column, selecting  > Edit.
- 5 Duplicates a selected notification configuration. You can also duplicate a configuration by selecting a configuration and then in the Actions column, selecting  > Duplicate.
- 6 Displays the following options:
  - **Import:** Imports a notification server, type, or template. For example, on the Servers tab, you can import a notification server configuration.
  - **Export All:** Exports all of the configurations. For example, if you are on the Servers tab, you can export all of the notification server configurations.
  - **Export:** Exports a selected configuration. You can also export a configuration by selecting a configuration and then in the Actions column, selecting  > Export.
- 7 Filters by Email, SNMP, Syslog, or Script.
- 8 Searches configurations in the grid.

## Templates Tab

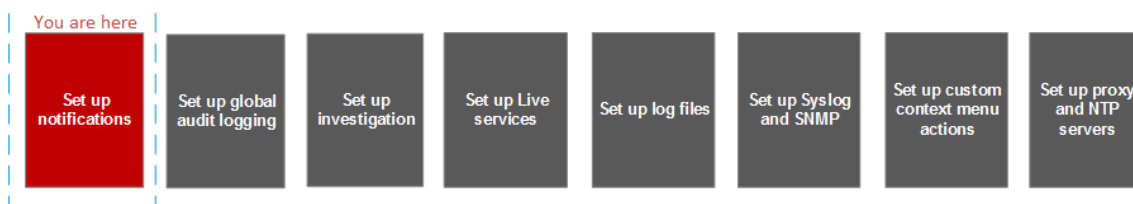
The Notification Templates tab enables to configure notification templates. Global Notifications configurations define notifications settings for Event Source Management (ESM), Health and Wellness, Global Audit Logging, Event Stream Analysis (ESA), and RESPOND. Notification templates define the format and message fields of the notifications.

Select a default template or configure templates for Email, SNMP, Syslog, and Script, depending on the template type. For Event Stream Analysis (ESA) templates, configure Email, SNMP, Syslog, and Script. For Audit Logging templates, configure Syslog.

Event Stream Analysis templates are not specific to any type of alert notifications, that is, the same template can be used for all types of notifications.

When upgrading from NetWitness Suite 10.4, all existing notification templates migrate to the Event Stream Analysis template type.

### Workflow



### What do you want to do?

Role	I want to ...	Show me how
Administrator	Define notification Templates	<a href="#">Configure Templates for Notifications</a>

### Related Topics

[Configure Global Notifications Templates](#)

[Configure a Template](#)

[Define a Template for ESA Alert Notifications](#)

[Delete a Template](#)

[Duplicate a Template](#)

[Edit a Template](#)


[Import and Export a Global Notifications Template](#)

### Quick look

The following example illustrates Global Notification Templates Tab.

The screenshot displays the 'Global Notifications' configuration page in the RSA NetWitness Suite. The page is divided into a left-hand navigation menu and a main content area. The main content area is titled 'Global Notifications' and contains a table of templates. The table has four columns: 'Name', 'Template Type', 'Description', and 'Actions'. The 'Name' column contains various template names, the 'Template Type' column lists categories like 'Audit Logging' and 'Event Stream Analysis', the 'Description' column provides details for each template, and the 'Actions' column contains a gear icon for each row. Red arrows and numbers 1 through 5 are overlaid on the image to highlight specific UI elements: 1 points to the toolbar, 2 points to the 'Name' column header, 3 points to the 'Template Type' column header, 4 points to the 'Description' column header, and 5 points to the 'Actions' column header.

Name	Template Type	Description	Actions
Default Audit CEF Template	Audit Logging	Default Audit CEF Template	[Gear]
Default Audit Human-Readable Format	Audit Logging	Default Audit Human-Readable Format	[Gear]
Default SMTP Template	Event Stream Analysis	Default SMTP Template	[Gear]
Default SNMP Template	Event Stream Analysis	Default SNMP Template	[Gear]
Default Script Template	Event Stream Analysis	System default FreeMarker template for Scri...	[Gear]
Default Syslog Template	Event Stream Analysis	Default Syslog Template	[Gear]
ESM Default Email Template	Event Source Monitoring	ESM Default Email Template	[Gear]
ESM Default SNMP Template	Event Source Monitoring	ESM Default SNMP Template	[Gear]
ESM Default Syslog Template	Event Source Monitoring	ESM Default Syslog Template	[Gear]
Health & Wellness Default SMTP Template	Health Alarms	Health & Wellness Default SMTP Template	[Gear]
Health & Wellness Default SNMP Template	Health Alarms	Health & Wellness Default SNMP Template	[Gear]

- 1 Selects a row for an action in the toolbar. Selecting the check box in the column title selects or deselects all rows in the grid.
- 2 Identifies or labels the templates
- 3 Choose a Template Type
- 4 Describes the templates
- 5 Provides an Actions menu  for the selected templates with actions that can be taken on the Templates. The Actions menu enables you to delete, edit, duplicate, and export the configuration.



## HTTP Proxy Settings Panel

HTTP Proxy Settings Panel introduces the proxy support features of the Administration System view > HTTP Proxy Settings panel.

**Note:** Proxy support is only for HTTP and HTTPS proxies and not SOCKS5.

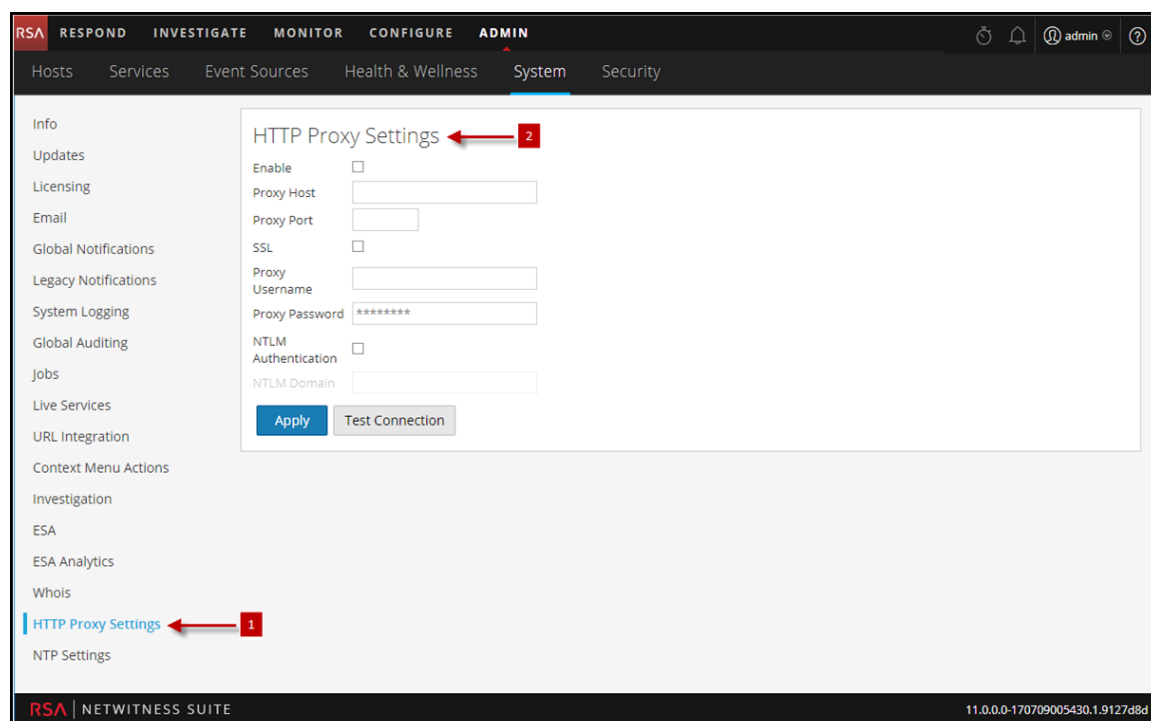
The HTTP Proxy Settings panel provides a user interface for configuring a proxy for use across NetWitness Suite modules and services. The Proxy Settings set up a proxy to be used wherever a proxy is needed in NetWitness Suite. The settings in this panel override any proxy settings configured for an individual service such as Malware Analysis or Live.

## Related topics

[Configure Proxy for NetWitness Suite](#)

## Quick Look

The following example illustrates an HTTP Proxy Settings Panel.



**1** Displays the HTTP Proxy Settings Panel.

**2** Allows the user to configure HTTP Proxy Settings.

## Toolbar and Features

This table describes the features in the Proxy Settings section.

Feature	Description
<b>Enable</b>	Enable the system proxy configuration for use in NetWitness Suite.
<b>Proxy Host</b>	The hostname for the proxy host.
<b>Proxy Port</b>	The port used for communication on the proxy host.
<b>Proxy Username</b>	(Optional) The user name used to log on to the proxy host if the proxy requires authentication.
<b>Proxy Password</b>	(Optional) The user password used to log on to the proxy host if the proxy requires authentication.
<b>Use NTLM Authentication</b>	Use NT LAN Manager authentication and session security protocols.
<b>NTLM Domain</b>	The name of NTLM domain.
<b>Use SSL</b>	(Optional) Enable communication using SSL.
<b>Apply</b>	Applies any changes made, and they become effective immediately.

## Email Configuration Panel

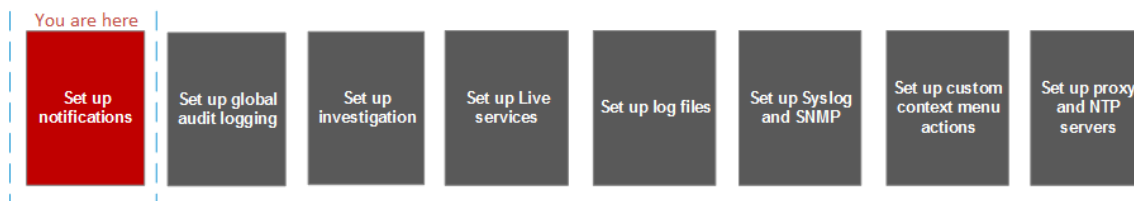
The Email Configuration Panel provides information about email configuration settings in the System View > Email Configuration panel. RSA NetWitness® Suitesends notifications to users via email about various system events. To be able to configure these email notifications, first configure the SMTP email server (See [Configure Email Servers and Notification Accounts](#)).

The Email Configuration panel provides a way to:

- Configure the email server.
- Set up an email account to receive notifications.
- View statistics on email operations.

## Workflow

This workflow shows the necessary procedures to configure and verify Email Panel.



## What do you want to do?

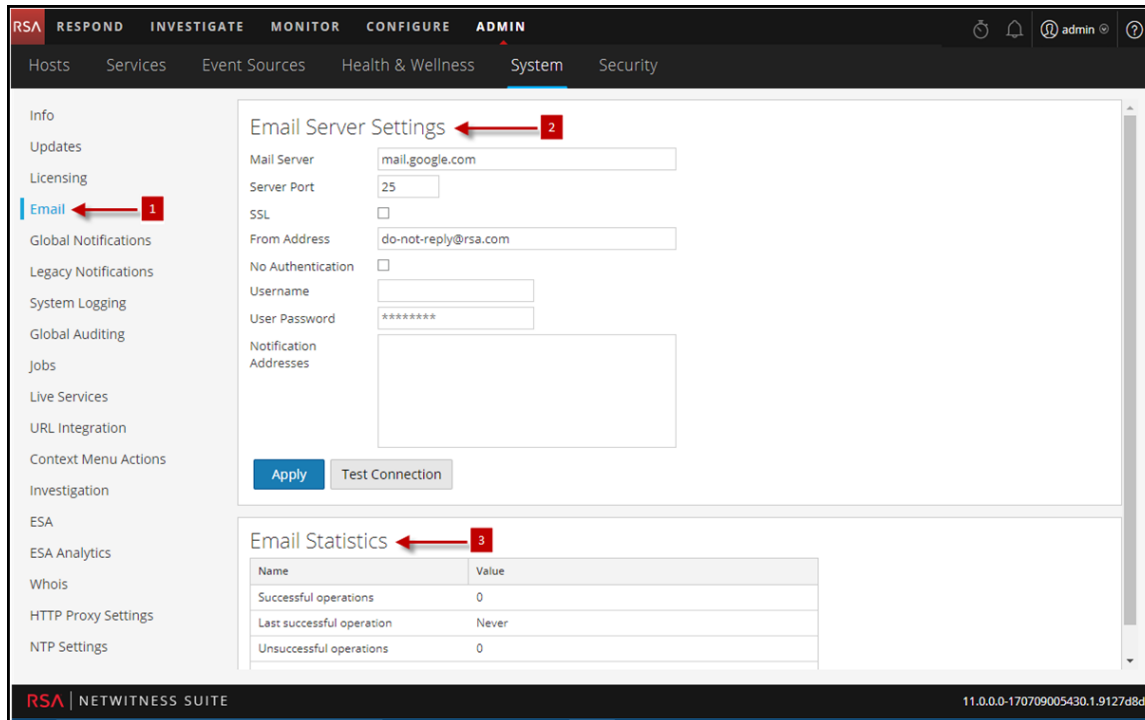
Role	I want to ...	Show me how
Administrator	Configure the SMTP Email Server	<a href="#">Configure Email Servers and Notification Accounts</a>
<b>Administrator</b>	<b>Email Setting as Notification Server</b>	<a href="#">Configure the Email Settings as Notification Server</a>
Administrator	Setup, Verify and Activate the Email Account	Receive Notification on Email

## Related Topics

- [Configure the Email Settings as Notification Server](#)
- [Configure Email as a Notification](#)
- [Configure Email Servers and Notification Accounts](#)

## Quick Look

The following example illustrates an Email configuration. The configuration defines how events are notified on Email.



- 1 Displays the Email Configuration Panel.
- 2 Allows the user to configure Email Server settings.
- 3 Provides feedback on Email operations.

## Toolbar and Features

The **Email Configuration** panel has two sections: **Email Server Settings** and **Email Statistics**.

### Email Server Settings

In the **Email Server Settings** section, you configure the following parameters.

Feature	Description
<b>Mail server</b>	The email server name. The default value is <b>mail.google.com</b> .
<b>Server port</b>	The server port used to send and receive emails. The default value is <b>25</b> .

Feature	Description
<b>Use SSL</b>	The preference for SSL use in communications between the email server and NetWitness Suite. The default value is to not use SSL (unchecked).
<b>From address</b>	The address that appears in all emails from NetWitness Suite. The default from address for emails is <b>do-not-reply@rsa.com</b> .
<b>Username</b>	The username to access the email server. The default value is <b>blank</b> .
<b>User password</b>	The user password to access the email server. The default value is <b>blank</b> .
<b>Test connection</b>	Tests the connection to the email server.
<b>Apply</b>	Applies the email configuration to this instance of NetWitness Suite.

## Email Statistics

The Email Statistics section provides feedback on the number of successful and failed email operations as well as the time of the last successful and unsuccessful email operation. For each statistic the name of the statistic and the value is displayed.

## ESA Settings Panel

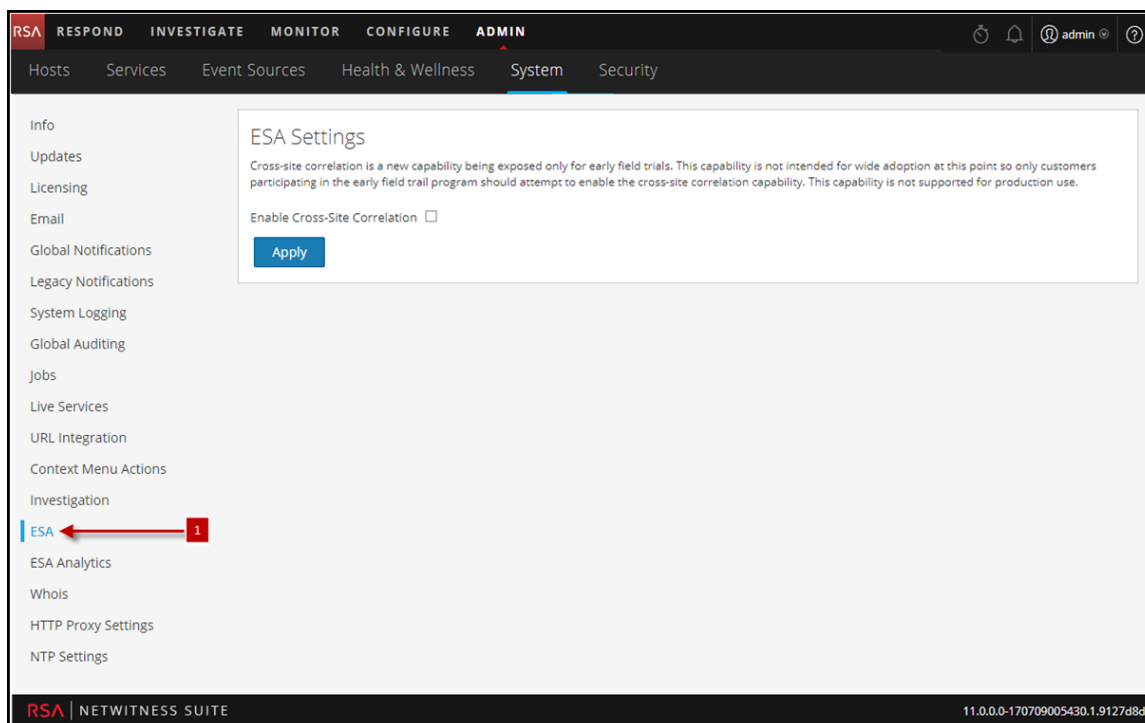
The ESA settings panel is where you enable and disable cross-site correlation. Cross-site correlation is a new capability being exposed only for early field trials. This capability is not intended for wide adoption.

**Caution:** Only customers participating in the early field trial program should attempt to enable the cross-site correlation capability. This capability is not supported for production use.

## Related Topics

- [Define a Template for ESA Alert Notifications](#)
- Investigation and Malware Analysis Guide
- Context Hub Configuration Guide

## Quick Look



- 1 Displays the ESA Setting Panel.

## Toolbar and Features

The features of the ESA Settings panel are:

- Enable Cross-Site Correlation checkbox: when checked enables cross-site correlation in ESA. When you add a deployment in ADMIN > Alerts > Configure, you can deploy the same rule set on multiple ESA services for centralized rules processing.
- Apply button: activates your selection.

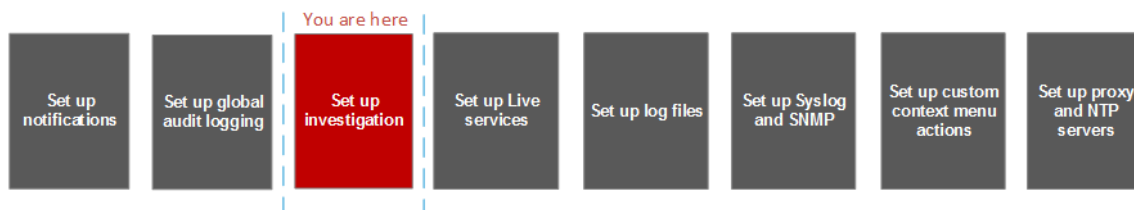
## Investigation Configuration Panel

The System view > Investigation Configuration panel, which provides the user interface for Administrators to configure the system-wide settings that NetWitness Suite Investigation uses when analyzing data and reconstructing an event.

The Investigation Configuration settings allow an administrator to manage application performance for Investigation. As analysts analyze and reconstruct sessions that they are investigating, performance can be affected by operations that involve loading, searching, visualizing, and reconstructing large amounts of data.

**Note:** Analysts can also set individual preferences for Investigation in the Profiles view and in the Navigation view.

## Workflow



## What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure navigate, events and context lookup settings	<a href="#">Configure Investigation Settings</a>
Administrator	Clear reconstruction cache for services	<a href="#">Configure Investigation Settings</a>

## Related Topics

- [Standard Procedures](#)

## Quick Look

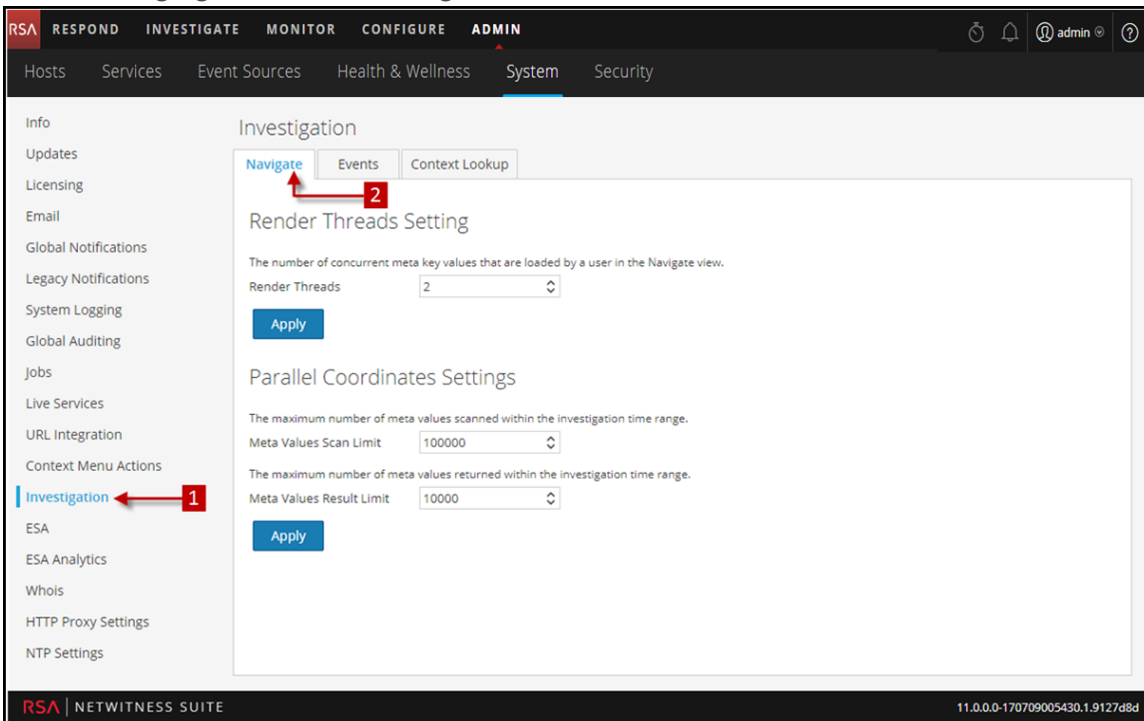
The Investigation Configuration panel has three tabs: Navigate, Events, and Context Lookup.

Though most fields in the tabs have a selection list with specific increments through the range of possible values, you can enter a value within the allowed range manually. An invalid entry is signaled by the field highlighted in red. When valid values are selected, clicking Apply in a given section puts the changes into effect immediately.



## Navigate Tab

The following figure shows the Navigate tab.



1 Displays the Investigation Configuration Panel.

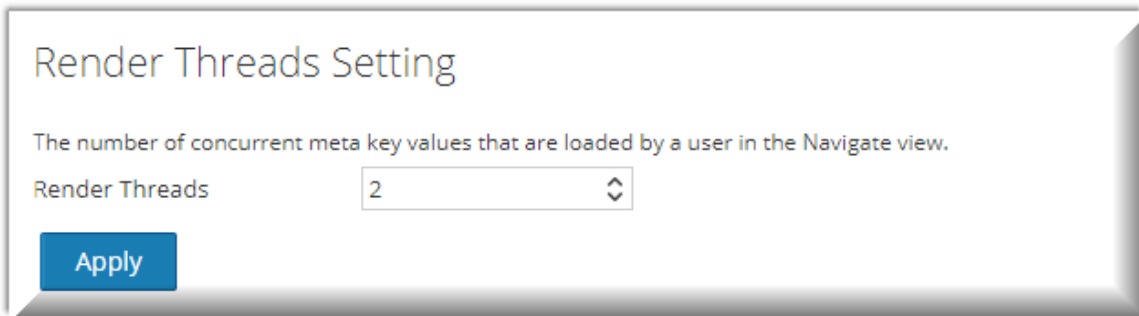
2 Displays the Navigate Tab.

## Toolbar and Features

The Navigate tab has two sections: Render Threads Setting and Parallel Coordinates Settings.

### Render Threads Setting

The Render Threads Setting is a selectable value between 1 and 20, which defines the number of concurrent (Values) loads in the Navigate view. The default value is 1.



### Parallel Coordinates Settings

The Parallel Coordinates Settings apply to the Parallel Coordinates visualization in the Navigate view. There is a fixed limit on the amount of data that can be rendered as a parallel coordinates chart. In NetWitness Suite the administrator can configure parallel coordinates limits here.

**Note:** For better performance, recommended settings are **Meta Values Scan Limit: 100000** and **Meta Values Result Limit: 1000-10000**.

Parallel Coordinates Settings

The maximum number of meta values scanned within the investigation time range.

Meta Values Scan Limit

The maximum number of meta values returned within the investigation time range.

Meta Values Result Limit

Apply

The following table describes the Parallel Coordinates Settings.

Parameter	Description
Meta Values Scan Limit	The maximum number of meta values scanned within the Investigation time range the analyst has selected in the Navigate view. Possible values are in the range of 1,000 to 10,000,000. The default value is 100,000.
Meta Values Result Limit	The maximum number of meta values returned within the Investigation time range the analyst has selected in the Navigate view. Possible values are in the range of 100 to 1,000,000,000. The default value is 10,000.

## Quick Look

### Events Tab

The following figure shows the Events tab.

Procedures associated with this panel are provided in [Standard Procedures](#).

**1** Displays the Investigation Configuration Panel.

**2** Displays the Events Tab.

## Toolbar and Features

The Events tab provides configurable settings that affect the investigation of events. This tab has four sections: Event Search Settings, Reconstruction Settings, Web View Reconstruction Settings, and Reconstruction Cache Settings.

### Event Search Settings

The Event Search Settings help to limit the number of events scanned when searching in the Events view.

The following table describes the Event Search Settings.

Parameter	Description
Events Scanned Limit	The maximum number of events to scan when searching in the Events view.
Events Result Limit	The maximum number of results to return when searching in the Events view.

## Reconstruction Settings

As analysts reconstruct sessions that they are investigating, some events can be very large and contain many thousands of source packets. Reconstructing these sessions, especially in a multi-user environment, can degrade application performance. The Reconstruction Settings allow an administrator to limit the number of packets and the size of a single event during reconstruction.

**Note:** An override to the Reconstruction Settings section is configurable for web views (under Web View Reconstruction Settings).

### Reconstruction Settings

Reconstructing events containing many thousands of packets can degrade application performance in a multi-user environment. These settings protect performance by placing limits on the amount of data processed in the reconstruction of a single event.

Max Packets:

Max Size (bytes):

Enabling this parameter allows any analyst to render full sessions using all available packets for that session bypassing the above global settings. The resources to provide this rendering are shared between users on the NetWitness server. Users trying to display sessions of large size or with a large amount of packets could effect not only their experience but other users of the system. To limit possible performance impact increasing the number of max packets used by default may be sufficient depending on analyst use case.

Allow Full Packet Reconstruction Override

Enabling this parameter allows NetWitness Server to read the HTML Page and parse the Charset from the Meta Tag if available. This allows NetWitness Server to correctly Encode the Non ASCII Characters correctly on UI while reconstructing the session as Text or Web Page. The parsing is done for rendering each request in a HTTP Session and can cause performance degradation for these reconstruction view.

Allow Parsing of HTML Charset for Web pages

### Web View Reconstruction Settings

Some web pages distribute supporting files such as images and cascaded style sheet (CSS) files across multiple web events. The reconstruction of the original target web page can be improved by scanning for related events and using those when reconstructing the original event.

Enable supporting files for web view (disabling supersedes user setting).

[Advanced Settings](#)

The following table describes the Reconstruction Settings features.

Parameter	Description
Maximum number of packets for a single event	<p>This setting protects performance by placing a limit on the number of packets processed for a single event reconstruction.</p> <p>Possible values are in the range from 100 to 10,000 packets, using manual entry or increments of 100 from the selection list. The default value is 100 packets.</p>
Maximum size, in bytes of a single event	<p>This setting protects performance by placing a limit on the maximum size, in bytes, of a single event reconstruction.</p> <p>Possible values are in the range from 102,400 to 104,857,600 bytes, using manual entry or increments of 10,240 from the selection list. The default value is 2,097,152 bytes.</p>
Allow Full Packet Reconstruction Override	<p>When this checkbox is selected, the analysts is provided with a Use More Packets button in the Reconstruction Panel. This enables the NW Server to regenerate events using all the packets available in the Event.</p>
Allow Parsing of HTML Charset for Web pages	<p>This option allows the NetWitness Server to identify the web page encoding defined in the HTML meta tag instead of the HTTP header. The default setting is disabled.</p>

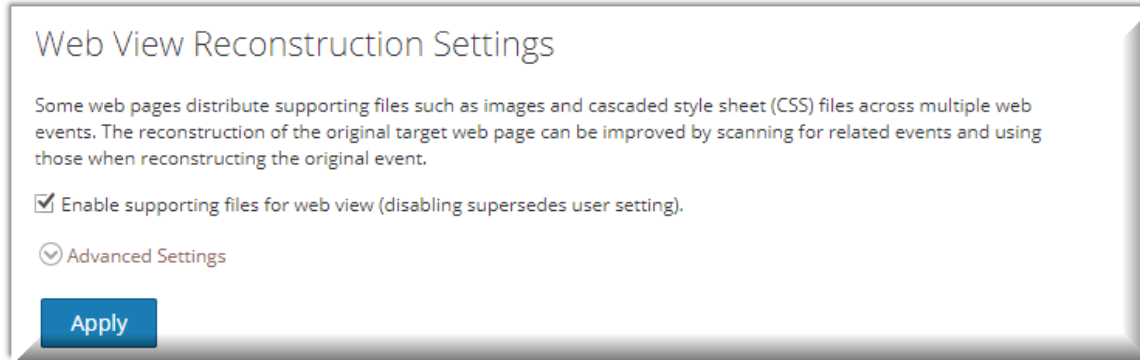
## Web View Reconstruction Settings

The Web View Reconstruction Settings allow an administrator to configure settings that improve the reconstruction of a web view by scanning and reconstructing related events that contain the same supporting files. When NetWitness Suite is reconstructing a web view that spans multiple events, it is possible to improve the reconstruction of the target event by scanning and reconstructing related events that contain the same supporting files, such as images and cascaded style sheet (CSS) files.

- The only related events scanned are HTTP service type events with the same source address as the target event, and a time stamp within a specified time range before and after the target event.

- The maximum number of related events to scan is configurable.

Clicking on the Advanced Settings option displays all configurable settings in this section.



The following table describes the Web View Reconstruction Settings.

Parameter	Description
Enable supporting files for web view	<p>This option determines how web views that have related data in other sessions are reconstructed. The default setting is enabled.</p> <p>When enabled, supporting files from related events can be used in the reconstruction of web views. Additional settings for calibrating the performance are enabled in this section, and Analysts have the option to enable CSS use in reconstructions.</p> <p>When disabled, supporting files from related events are not used and the setting for analysts to enable CSS use in reconstructions is disabled.</p>

Parameter	Description
Time Range to Scan Related Events	<p>Available when <b>Enable supporting files for web view</b> is checked.</p> <p>Configures the time range within which NetWitness Suite scans related events that are of the service type HTTP and have the same source address as the target event. This is a value between 0 and 60.</p> <ul style="list-style-type: none"><li>• Seconds Before Target Event</li><li>• Seconds After Target Event</li></ul>
Limit the number of related events processed	<p>Allows configuration of the maximum number of related events that NetWitness Suite scans within the specified time range to discover supporting files for the target event. By default, this is disabled. When enabled, the Maximum Related Events field becomes active.</p>
Max Related Events	<p>When <b>Limit the number of events processed</b> is enabled, this field specifies the maximum number of related events that NetWitness Suite scans within the specified time range to discover supporting files for the target event.</p> <p>This is a selectable value between 10 and 1,000, using an increment of 100. The default value is 100.</p>
Limit the number of packets and size of each related event	<p>Overrides the general settings for the maximum number of packets and maximum size (in bytes) for individual related events.</p>

Parameter	Description
Maximum Number of Packets for a Single Related Event	Possible values are in the range from 100 to 10,000 packets, using increments of 100 from the selection list. The default value is 100 packets.
Maximum Size, in Bytes, of a Single Related Event	Possible values are in the range from 102,400 to 104,857,600 bytes, using increments of 10,240 from the selection list. The default value is 524,288 bytes.

## Reconstruction Cache Settings

In some cases, the reconstruction cache can present incorrect content; for this reason NetWitness Suite removes reconstructions that are older than a day from the cache. The cache is cleaned every day at midnight. Between the daily cache cleanings, certain actions may result in stale cache being used for a reconstruction, and if the need arises, administrators can manually clear cache for one or more services that are connected to the current NetWitness Server.

<input type="checkbox"/>	Name ^	Address	Type
<input type="checkbox"/>	Archiver	10.31.125.242	Archiver
<input type="checkbox"/>	Broker	10.31.125.249	Broker
<input type="checkbox"/>	Broker	10.31.125.243	Broker
<input type="checkbox"/>	Broker	10.31.125.240	Broker
<input type="checkbox"/>	Concentrator	10.31.125.244	Concentrator
<input type="checkbox"/>	Decoder	10.31.125.245	Decoder
<input type="checkbox"/>	Log Decoder	10.31.125.246	Log Decoder
<input type="checkbox"/>	Workbench	10.31.125.242	Workbench

The following table describes the Reconstruction Cache Settings features.

Feature	Description
Selection box	Selection box in individual rows and in the title bar allow selection of one or more, or all services that need to have cache cleared manually.

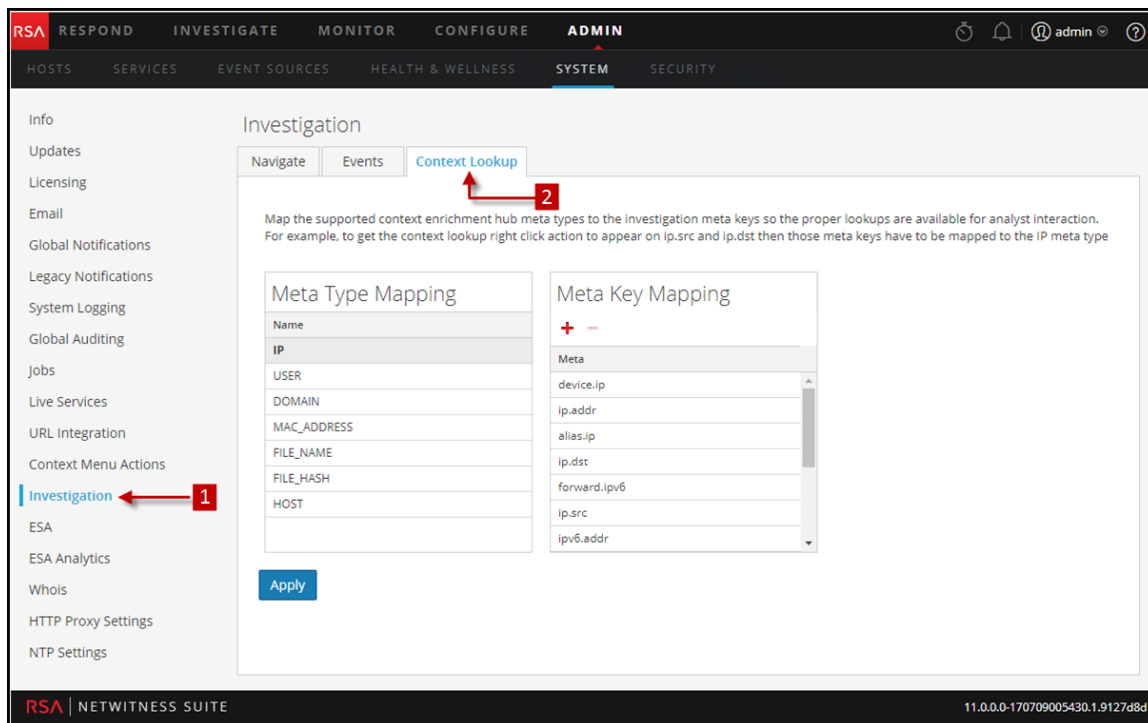


Feature	Description
Clear Cache for Selected Services	Clears the reconstruction cache for each selected service.
Clear Cache for All Services	Clears the reconstruction cache for all services.

## Quick Look

### Context Lookup Tab

The following figure shows the Context Lookup tab.



Procedures associated with this panel are provided in "Manage Meta Type and Meta Key Mapping" in the *Context Hub Configuration Guide*.



**1** Displays the Investigation Configuration Panel.

**2** Displays the Context Lookup Tab.

## Toolbar and Features

The Context Lookup tab enables the administrator to configure the Investigation meta keys and meta type mapping. The administrator can add or remove meta keys found in Investigation to the list of meta types supported by Context Hub service.

The following table describes the features of the Context Lookup tab.

Feature	Description
	Adds an meta key to the selected meta type supported by Context Hub.
	Deletes the meta key from the selected meta type.
Apply	Saves the changes made to the Context Lookup tab.

## Live Services Configuration Panel

Live Services Configuration Panel introduces the features for setting up your Live account and the CMS server connection.

Live Account consists of two sections, namely RSA Live Status and Download Live Feedback Activity Log. **Sign In** by entering your Live Account credentials to access the Live Services. To activate your Live account for NetWitness Suite, please contact RSA Customer Care. When you have confirmation that your Live account has been set up, you can configure the CMS server connection as described in [Configure Live Services Settings](#)

The Live Services panel provides the user interface for:

- The Live account
- The Live Content update schedule and preferences for notification of updates
- Participation in Live Feedback
- Sharing Live Content Usage Details
- RSA Live Connect (Beta)

## New Features Enabled Dialog

When you log onto NetWitness Suite for the first time, you will be prompted with **New Features Enabled** dialog.

Feature	Description
<b>Accept</b>	Clicking Accept indicates that you agree to the following: <ul style="list-style-type: none"><li>• Participate in Live Feedback</li><li>• Allow NetWitness Suite to send RSA the usage metrics and version of NW hosts about your environment to RSA, provided a Live Account is configured.</li><li>• Receive threat intelligence data from Live Connect.</li></ul>
<b>View Settings</b>	Clicking <b>View Settings</b> redirects you to the Live Services UI to view the settings. If you have not configured the Live Account, a masked screen is displayed.

For information on Live Feedback, see [Live Feedback Overview](#)

For information on Analyst Behaviors and Data Sharing, see the "**NetWitness Suite Feedback and Data Sharing**" topic in the *Live Services Management Guide*.

For information on Live Connect Threat Insights, see [Configure Live Services Settings](#)

## Workflow



## What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure Live Account, CMS Server Connection	<a href="#">Configure the Email Settings as Notification Server</a>
Administrator	Upload Data to RSA for Live Feedback	<a href="#">Upload Data to RSA for Live Feedback</a>
Administrator	Setup, Verify Live Service Configuration Panel	Live Services Configuration Panel
Administrator	Overview On Live Feedback	<a href="#">Live Feedback Overview</a>

## Related Topics

- [Live Feedback Overview](#)
- [Configure Live Services Settings](#)
- [Upload Data to RSA for Live Feedback](#)
- Live Services Management Guide

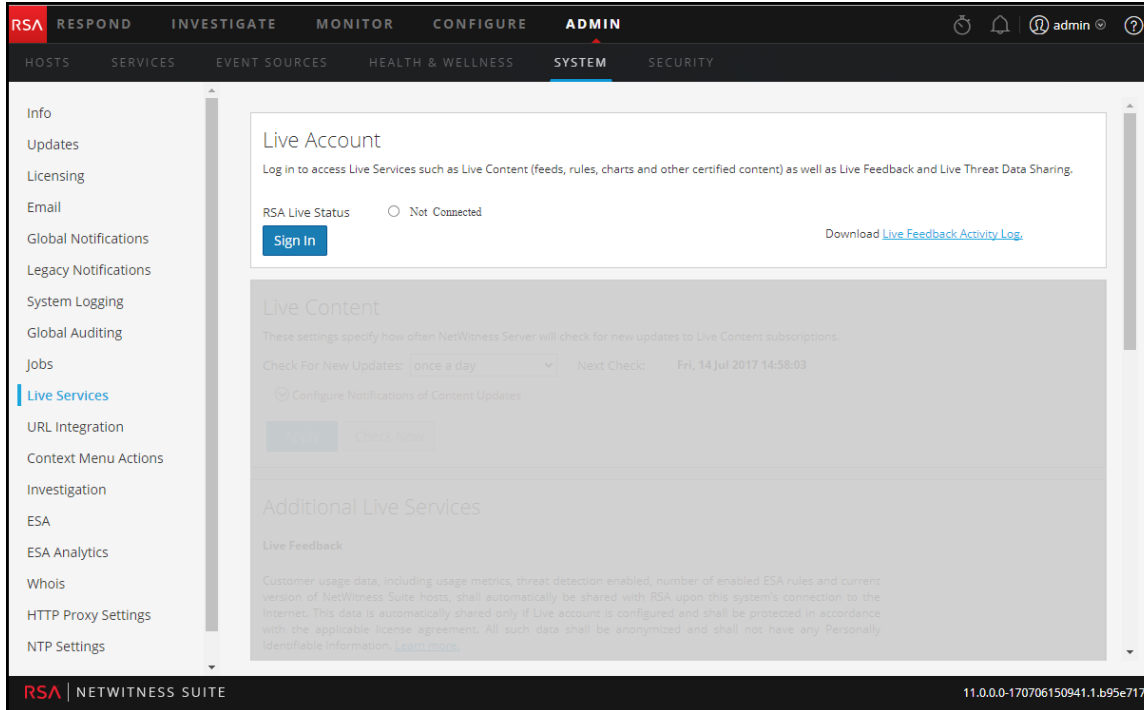
## Live Services Quick Look

You access this view in the **ADMIN > SYSTEM > Live Services**.

The screenshot displays the RSA NetWitness Suite Admin console. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The 'ADMIN' section is active, showing a sub-menu with 'Hosts', 'Services', 'Event Sources', 'Health & Wellness', 'System', and 'Security'. The 'System' sub-menu is expanded, and 'Live Services' is selected, indicated by a red arrow and the number 1. The main content area is divided into three sections: 'Live Account' (indicated by a red arrow and the number 2), 'Live Content' (indicated by a red arrow and the number 3), and 'Additional Live Services' (indicated by a red arrow and the number 4). The 'Live Account' section shows the user is 'Connected' and provides a 'Modify' button. The 'Live Content' section shows update frequency settings set to 'once a day' and a 'Check Now' button. The 'Additional Live Services' section includes a 'Live Feedback' section with a disclaimer about data sharing.

**Note:** If you are not signed in with your Live Account credentials, a masked screen is displayed.

- 1 Displays the Live Services Configuration Panel
- 2 Enter Live Account Credentials With the Help of Customer Care.
- 3 Provides Update On Live Content
- 4 Additional Live Services Provides Live Feedback



## Toolbar and Features

The Live Configuration panel has three sections: Live Account, Live Content, and Additional Live Services.

### Live Account Section

In the **Live Account** section, you must enter the Live credentials. The information needed to set up the user's Live account consists of the Username, Password, and Live URL for the RSA Content Management System. This information is provided by Customer Care.

The following table describes the Live Account section features.

Feature	Description
<b>Host</b>	The Live URL for the Content Management System. The default value points to the RSA CMS at <b>cms.netwitness.com</b> .
<b>Port</b>	The communications port for Live to send requests to the Content Management System. The default value for this field is <b>443</b> , which is the communications port on the Content Management System.
<b>SSL</b>	Allows the user to communicate via SSL.
<b>Username</b>	The Live account user name as provided by RSA Customer Care.
<b>Password</b>	The Live account user password as provided by RSA Customer Care.

Feature	Description
<b>Test connection</b>	Tests if the connection is successful or not.
<b>Apply</b>	Saves and applies the configuration.

The Live Account section, provides an option to download and share the Live Feedback historical data by clicking Live Feedback Activity Log.

For more information about how to download historical data, see [Upload Data to RSA for Live Feedback](#)

## Live Content Section

You can configure the Live Content Synchronization interval and notification at which NetWitness Suite checks for new updates to Live Content:

Use the **Check for New Updates** field to change the interval. Select an interval from the drop-down list. The default value for this setting is **once a day**.

### Live Content

These settings specify how often NetWitness Server will check for new updates to Live Content subscriptions.

Check For New Updates:  Next Check: Thu, 18 Aug 2017 05:05:12

Configure Notifications of Content Updates

E-Mail addresses specified here will receive messages containing a list of subscribed resources that have been updated in the last 24hrs.

Email Addresses

HTML Format

The following table describes the Live Content features.

Feature	Description
<b>Check for new updates</b>	<p>This setting dictates how often NetWitness Suite checks for new updates to Live Subscriptions and synchronizes subscribed resources and tags:</p> <ul style="list-style-type: none"> <li>• once a day</li> <li>• twice a day</li> <li>• four times a day</li> <li>• every hour</li> <li>• every other hour</li> <li>• every half hour</li> </ul> <p>The default value for this setting is once a day.</p>
<b>Next Check</b>	Displays the time and date of the next scheduled Live synchronization based on the configured interval for checking.
<b>Email Addresses</b>	Email addresses specified here receive messages containing a list of subscribed resources that have been updated in the last 24 hours.
<b>HTML format</b>	<p>Specifies the format of email messages.</p> <ul style="list-style-type: none"> <li>• Checked = HTML</li> <li>• Not checked = text</li> </ul>
<b>Check Now</b>	<p>Instead of waiting for the next scheduled resource cycle, this option forces Live to begin immediate synchronization of the subscribed resources in this instance of NetWitness Suite.</p> <div style="border: 1px solid yellow; padding: 5px;"> <p><b>Caution:</b> Use this feature with caution because synchronization can cause a parser reload if a Lua Parser or Flex Parser is deployed in the update cycle. This is acceptable once or twice a day, but a number of back-to-back parser reloads can cause packet loss at the Decoder. If this is the initial setup and you haven't configured Live resource subscriptions, do not Synchronize Now. Wait until you have configured subscriptions.</p> </div>
<b>Apply</b>	<p>Applies the changed configuration to the subscription synchronization behavior. The changes become effective immediately. The <b>Next Live synchronization is scheduled for</b> field is updated if the time changed.</p>

## Force Immediate Synchronization



To force immediate synchronization, click **Check Now**. NetWitness Suite checks for updates in subscribed resources.

Instead of waiting for the next scheduled resource cycle, this option forces Live to begin immediate synchronization of the subscribed resources in this instance of NetWitness Suite. One use for this is to see the immediate impact of a configuration change. For example, a new service has been added, or new resources have been toggled for automatic deployment. The scheduled synchronization could take place hours later if Live Services is set to synchronize a few times a day.

**Caution:** Synchronization can cause a parser reload if a Flex Parser is deployed in the update cycle. This is acceptable once or twice a day, but a number of back-to-back parser reloads can cause packet loss at the Decoder. If this is the initial setup and you haven't configured Live resource subscriptions, do not Synchronize Now. Wait until you have configured subscriptions.

## Additional Live Services

## Additional Live Services

### Live Feedback

Customer usage data, including usage metrics, threat detection enabled, number of enabled ESA rules and current version of NetWitness Suite hosts, shall automatically be shared with RSA upon this system's connection to the Internet. This data is automatically shared only if Live account is configured and shall be protected in accordance with the applicable license agreement. All such data shall be anonymized and shall not have any Personally Identifiable Information. [Learn more.](#)

**Share Live Content Usage Details**

Live Content (All Resource Types) usage metrics shall be automatically shared with RSA upon this system's connection to the Internet and if the Live Account is configured. This data will be leveraged for deep analysis to improve and optimize the use of Live Content. Customers who wish not to share data, should change their setting. All data collected shall be protected in accordance with the applicable license agreement. All such data shall be anonymized and shall not have any Personally Identifiable Information. [Learn more.](#)

### RSA Live Connect (Beta)

RSA Live Connect is a cloud based threat intelligence service. This service collects, analyzes, and assesses threat intelligence data such as IP addresses, domains, and files collected from various sources including the RSA NetWitness Suite and RSA NetWitness Endpoint customer community. The RSA Live Connect cloud service stores this information in a secure environment and provides an anonymous, secure 2-way channel over SSL between the RSA Live Connect cloud and the RSA NetWitness Suite/RSA NetWitness Endpoint customers to share and monitor de-identified and obfuscated threat intelligence. This threat intelligence information can be leveraged by analysts for identifying and investigating potential security threats. [Learn more.](#)

Enable **Analyst Behaviors**  Not Connected

This Live Connect option is an automated data collection service. It is responsible for gathering meta data captured locally by NetWitness Suite and securely sending it to RSA Live Connect. This data will be leveraged for deep analysis to drive and improve the RSA Live and Live Connect threat intelligence services in order to proactively identify potential security threats.

*NOTE: The type of data that potentially could be shared from a user's network to the RSA Live Connect cloud service could encompass various types of meta data captured by the NetWitness Suite product such as ip.src, ip.dst, ip.addr, device.ip, alias.ip, alias.host, paddr, sessionid, domain.dst, domain.src.*

Customers who do not wish to receive threat intelligence and/or share de-identified and anonymized information with the Live Connect service should change their settings in the [Live Connect](#) feature and/or contact RSA Customer Support for more information.

Apply

**Note:** Click on Learn more to know more about the data RSA is collecting. For more information, see [Live Feedback Overview](#)

The following tables describes the Additional Live Services features.

Feature	Description
Live Feedback	<p>Lists the types of data RSA is collecting:</p> <ul style="list-style-type: none"> <li>• Product Name</li> <li>• Product Version</li> <li>• Product Instance</li> <li>• Activation Key</li> <li>• Details of each Component such as: <ul style="list-style-type: none"> <li>• ID</li> <li>• Name</li> <li>• Version</li> <li>• Instance ID</li> </ul> </li> <li>• Metrics for each component</li> </ul>
Share Live Content Usage Details)	Enables NetWitness Suite to send anonymous, technical data about the content usage metrics to RSA. This option is enabled by default.
RSA Live Connect	Provides more information about Live Connect service and configuring Live Services.
<b>Enable</b> (Threat Insights)	<p>Enables Threat Insights feature where Live Connect is added as a data source for Context Hub service and the analyst can pull threat intel data during investigation. Ensure that context hub is already configured before enabling this feature.</p> <p>This option is enabled by default (checked)</p>
<b>Enable</b> (Analyst Behaviors)	Enables NetWitness Suite to send anonymous, technical data about your environment to RSA. This option is enabled by default (checked)

Feature	Description
Apply	<p>Applies the configured changes. The changes become effective immediately.</p> <div data-bbox="576 373 1289 472" style="border: 1px solid green; padding: 5px;"><p><b>Note:</b> This option is applicable only for Threat Insights and Analyst Behaviors.</p></div>

## About Live Feedback Participation

When you participate in Live Feedback, it collects relevant information for further improvement. For information on Live Feedback, see [Live Feedback Overview](#).

When you install NetWitness Suite, you will be prompted to participate in Live Feedback. For information, see [Configure Live Services Settings](#)

If needed, you can manually download historical usage data and share it with RSA. For information on how to download historical usage data and share it with RSA, see [Upload Data to RSA for Live Feedback](#).

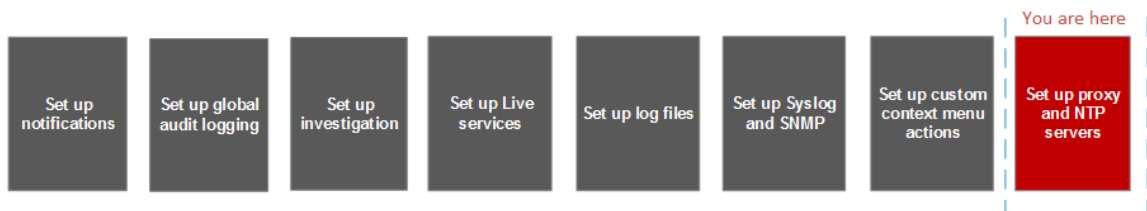
## NTP Settings Panel

NTP setting panel is a protocol designed to synchronize the host machine clocks over a network. For more information on NTP see their home page (<http://www.ntp.org/>).

**Note:** NetWitness Suite core hosts must be able to communicate with the NW host with UDP port 123 for NTP time synchronization.

You use the **ADMIN > System > NTP Settings** view to configure one or more NTP servers. After you configure an NTP server, NetWitness Suite uses NTP to synchronize the host machine clocks. You configure multiple NTP servers for Fail Over purposes.

## Workflow



## What you need to do?

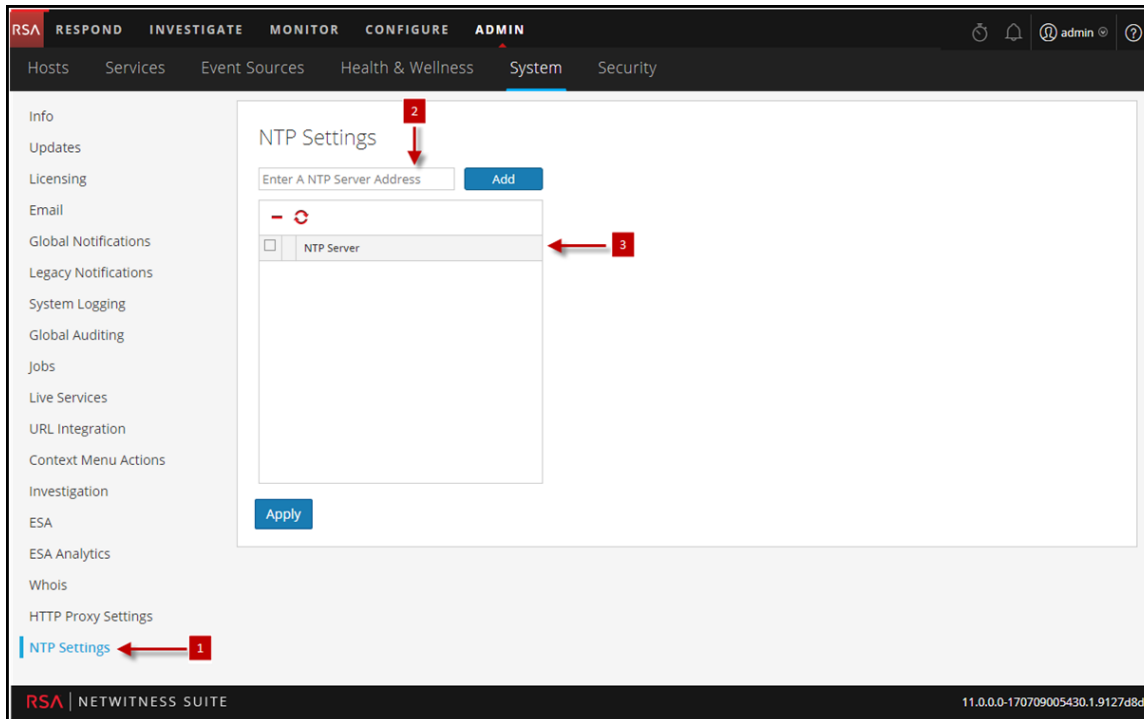
Role	I want to ...	Show me how
Administrator	Add or Modify an NTP Server	<a href="#">Configure NTP Servers</a>

## Related Topics

- [Configure NTP Servers](#)
- [Troubleshooting NTP Server Configuration](#)

## Quick Look




The following example illustrates an NTP setting panel. The panel defines how to add NTP server to NTP setting panel.



- 1 Displays the NTP setting panel
- 2 Enter the NTP Server IP Address or hostname.
- 3 click on an existing hostname

## Toolbar and Features

The following table describes the settings in the NTP Settings panel.

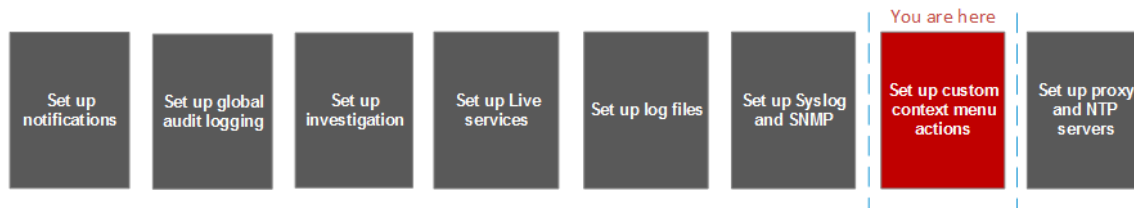
Setting	Description
	Enter the NTP Server IP Address or hostname.
<b>Add</b>	Adds the NTP server to NetWitness Suite.
	Delete the selected NTP server.
	Synchronizes the selected NTP server.
	Selects the NTP server that you want to delete or synchronize.

Setting	Description
NTP Server	<p>NTP Server IP Address or hostname. If you click on an existing hostname, NetWitness Suite makes the hostname editable and displays the following command buttons:</p> <ul style="list-style-type: none"><li>• <b>Update</b> - Applies your edits.</li><li>• <b>Cancel</b> - Cancels your edits.</li></ul>
<b>Apply</b>	Applies the NTP server settings and synchronizes host machine clocks to NTP.

## Context Menu Actions Panel

In the Context Menu Actions panel, Administrators can view built-in context menu actions, and add, edit, or delete custom context menu actions that appear as options in a context menu.

### Workflow



### What do you want to do?

Role	I want to ...	Show me how
Administrator	Custom Context Menu Actions panel	<a href="#">Add Custom Context Menu Actions.</a>

### Related Topics

- [Add Custom Context Menu Actions](#)

### Quick Look

The following figure is an example of the Context Menu Actions panel.



The screenshot shows the RSA NetWitness Suite Admin console. The left sidebar contains a navigation menu with 'Context Menu Actions' highlighted. A red box labeled '1' points to this menu item. The main content area displays the 'Context Menu Actions' panel, which includes a toolbar with icons for Add (+), Edit (pencil), Delete (-), and Refresh (circular arrow). A red box labeled '2' points to this toolbar. Below the toolbar is a table with the following columns: Menu Item, Id, Version, Type, Modules, and CSS Classes. The table lists various actions such as 'Host Profile Report', 'Suspicious VPN Session Report', 'Context Lookup', 'Add/Remove from List', 'Copy', 'Event Reconstruction', 'Event Analysis', 'Apply Drill in New Tab', 'Apply IEQUALS Drill in New Tab', 'Apply IEQUALS Drill', 'Open in New Tab', 'Geo-map Locations in New Tab', 'Live Lookup', 'Change Selected to Open', 'Change Selected to Closed', 'Change Selected to Auto', 'Change Selected to Hidden', and 'Refocus Investigation in New Tab'.

Menu Item	Id	Version	Type	Modules	CSS Classes
<input type="checkbox"/> Host Profile Report	viewInHostProfileRep...	1	UAP.common.contextmen...	investigation	ip-src, ip-dst, ip.src, ip.dst, i...
<input type="checkbox"/> Suspicious VPN Session Report	viewInVPNSessionRep...	1	UAP.common.contextmen...	investigation	username, user.src, user.d...
<input type="checkbox"/> Context Lookup	contextServiceDefault...	1	UAP.common.contextmen...	investigation	device-ip, eth-dst, domain-...
<input type="checkbox"/> Add/Remove from List	addToList	1	UAP.common.contextmen...	investigation	meta-value-name-link, nw-...
<input type="checkbox"/> Copy	copyMetaAction	1	UAP.common.contextmen...	investigation	meta-value-name-link, nw-...
<input type="checkbox"/> Event Reconstruction	reconstructionAction	1	UAP.common.contextmen...	investigation	x-grid-row
<input type="checkbox"/> Event Analysis	reconAnalysisAction	1	UAP.common.contextmen...	investigation	x-grid-row
<input type="checkbox"/> Apply Drill in New Tab	drillDownNewTabEqu...	1	UAP.common.contextmen...	investigation	meta-value-name-link
<input type="checkbox"/> Apply IEQUALS Drill in New Tab	drillDownNewTabNot...	1	UAP.common.contextmen...	investigation	meta-value-name-link
<input type="checkbox"/> Apply IEQUALS Drill	drillDownNotEquals	1	UAP.common.contextmen...	investigation	meta-value-name-link
<input type="checkbox"/> Open in New Tab	viewListNewTab	1	UAP.common.contextmen...	investigation	meta-value-session-link
<input type="checkbox"/> Geo-map Locations in New Tab	viewGeoMapNewTab	1	UAP.common.contextmen...	investigation	meta-value-geo-map-link
<input type="checkbox"/> Live Lookup	defaultLiveMenuOption	1	UAP.common.contextmen...	investigation	meta-value-name-link, nw-...
<input type="checkbox"/> Change Selected to Open	change-meta-view-AC...	1	UAP.common.contextmen...	investigation	metaGroupLanguagesGrid
<input type="checkbox"/> Change Selected to Closed	change-meta-view-AC...	1	UAP.common.contextmen...	investigation	metaGroupLanguagesGrid
<input type="checkbox"/> Change Selected to Auto	change-meta-view-AC...	1	UAP.common.contextmen...	investigation	metaGroupLanguagesGrid
<input type="checkbox"/> Change Selected to Hidden	change-meta-view-AC...	1	UAP.common.contextmen...	investigation	metaGroupLanguagesGrid
<input type="checkbox"/> Refocus Investigation in New Tab	rootDrill	1	UAP.common.contextmen...	investigation	meta-value-name-link

1 Displays the Context Menu Actions Panel

2 Toolbar allows the user to Add, Edit, Delete Context Menu Actions

## Toolbar and Features

The Context Menu Actions panel has a grid and a toolbar. The following table describes the toolbar options and grid features.

Features	Description
	Displays the Context Menu Configuration dialog, in which you can create a new context action.
	Refreshes the list.
	Deletes the selected context actions. NetWitness Suite does not request confirmation that you want to delete the action. The selected actions are immediately deleted with no opportunity to cancel.
	Displays the Edit Context Action dialog, in which you can edit an existing context action.

Features	Description
<b>Menu Item</b>	<p>The menu item as it appears in the context menu.</p> <p>When creating a context menu action, the parameter is <code>displayName</code>.</p> <p>Here is a line of sample code:</p> <pre>"displayName": "User Agent String Lookup"</pre>
<b>ID</b>	<p>The unique ID for the context action. When creating a context menu action, the parameter is <code>id</code>.</p> <p>Here is a line of sample code:</p> <pre>"id": "UserAgentStringAction"</pre>
<b>Version</b>	<p>The version number of the context action. When creating a context menu action, the parameter is <code>version</code>.</p> <p>Here is a line of sample code:</p> <pre>"version": "1"</pre>
<b>Type</b>	<p>The type of context action.</p> <p>When creating a context menu action, the parameter is <code>type</code>. All NetWitness Suite context action types begin with this string:</p> <pre>UAP.common.contextmenu.actions.</pre> <p>The last part of the string identifies the menu within NetWitness Suite, for example, <code>URLContextAction</code> or <code>LivePostContextAction</code>.</p> <p>Here is a line of sample code:</p> <pre>"type": "UAP.common.contextmenu.actions.URLContextAction"</pre>
<b>Modules</b>	<p>The names of the modules in which the context action is available. Currently all built-in context menu actions are for the Investigation module.</p> <p>When creating a context menu action, the parameter is <code>modules</code>.</p> <p>Here is a line of sample code:</p> <pre>"modules": [     "investigation" ],</pre>

Features	Description
<b>Module Classes</b>	<p>The CSS classes that identify the names of the module views in which the context action is available. Currently all built-in context menu actions are for the Investigation module and the non-meta key module classes are described in detail below.</p> <p>Here are a few lines of sample code:</p> <pre>"moduleClasses": [     "UAP.investigation.navigate.view.NavigationPanel", &lt;-- Enabled in Navigate pane--&gt;     "UAP.investigation.events.view.EventGrid" ],</pre>
<b>CSS Classes</b>	<p>The CSS classes to which the context menu action applies. The CSS classes define where the context menu shows up inside investigation when you right-click. When creating a context menu action, the parameter is <code>cssClasses</code>.</p> <p>Here is a line of sample code:</p> <pre>"cssClasses": [     "client" ]</pre> <p>Most of the CSS Classes that you can add are meta keys. You can also add certain non-meta key CSS classes. See additional details and examples below.</p>

## CSS Classes and Examples

CSS classes can be meta keys and non-meta keys.

### Meta Key CSS Classes

One type of CSS class that you can add is meta keys. For meta keys that have a period, change the period to a dash when defining a CSS class. For example, the meta key `alias.host` becomes the CSS class `alias-host`. The meta key `ip.src` becomes the CSS class `ip-src`.

### Non-Meta Key CSS Classes

Built-in non-meta key CSS Classes are also available. The classes in the following table define actions and the part of the user interface where the action is available.

CSS Class	Type	Description
meta-value-session-link	Action	Open on meta session count number
meta-value-name-link	Action	Open on meta value name
nw-event-value	Action	Use for reconstruction context actions on meta value
UAP.investigation.navigate.view. NavigationPanel	User interface	Applies to Navigate view
UAP.investigation.events.view. EventGrid	User interface	Applies to Event View
UAP.investigation.reconstruction.view. content.ReconstructedEventDataGrid	User interface	Applies to Event Reconstruction View

## Example

This is a commented example of a context menu action to validate the user agent from the Client Application (client) meta key. The comments are removed automatically once applied in the Administration System view. The new menu item is displayed after restarting the browser.

```
{
  "displayName": "User Agent String Lookup", <!-- What name shows up
in NW UI -->
  "cssClasses": [
    "client" <!-- What meta key to launch from -->
  ],
  "description": "",
  "type": "UAP.common.contextmenu.actions.URLContextAction",
  "version": "1",
  "modules": [
    "investigation"
  ],
  "local": "false",
  "groupName": "externalLookupGroup", <!-- What group to show link
in. Remove line to show in main list -->
  "urlFormat": "http://www.useragentstring.com/?uas={0}&getText=all", <!-- The
{0} gets replaced with whatever was right clicked on -->
  "disabled": "",
```

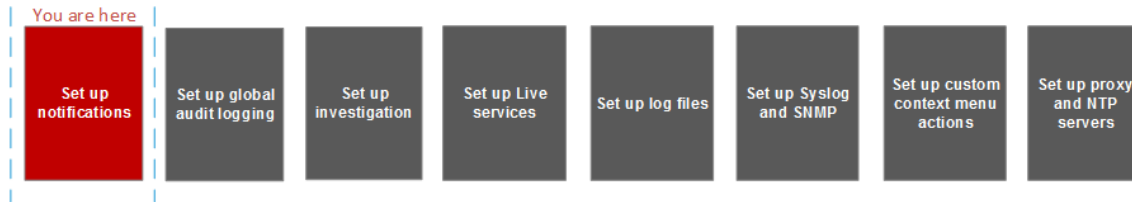
```
    "id": "UserAgentStringAction",
    "moduleClasses": [
      "UAP.investigation.navigate.view.NavigationPanel", <-- Enabled
in Navigate pane-->
      "UAP.investigation.events.view.EventGrid" <-- Enabled in Event
View pane -->
    ],
    "openInNewTab": "true",
    "order": "15"
  }
```

## Legacy Notifications Configuration Panel

The Legacy Notifications Configuration panel provides the ability to configure syslog and SNMP notification settings. These configurations are used for Entitlement, legacy Event Source Management (ESM), Warehouse Connector monitoring, and Archiver monitoring.

Procedures related to these settings are described in [Configure Syslog and SNMP Settings](#).

## Workflow



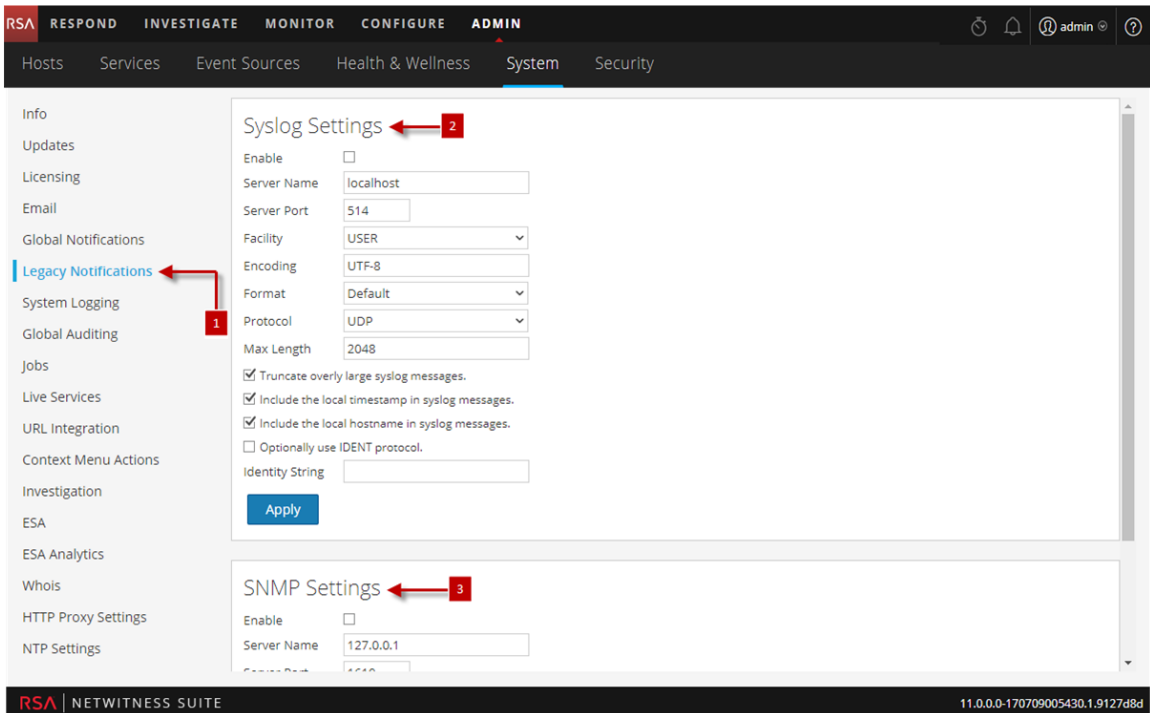
## What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure Syslog Settings	<a href="#">Configure Syslog and SNMP Settings</a>
Administrator	Configure SNMP Settings	<a href="#">Configure Syslog and SNMP Settings</a>

## Related Topics

- [Configure Syslog and SNMP Settings](#)

## Quick Look



- 1 Displays the Legacy Notification Configuration Panel.
- 2 Allows the user to configure syslog notifications for Entitlement, legacy Event Source Management (ESM), Warehouse Connector monitoring, and Archiver monitoring.
- 3 Allows the user to configure SNMP notifications for Entitlement, legacy Event Source Management (ESM), Warehouse Connector monitoring, and Archiver monitoring.

## Toolbar and Features

The Legacy Notifications Configuration Panel consists of two sections: Syslog Settings and SNMP Settings.

### Syslog Settings

The following table describes the available options for configuring syslog notifications for Entitlement, legacy Event Source Management (ESM), Warehouse Connector monitoring, and Archiver monitoring.

Feature	Description
<b>Enable</b>	Enables the syslog settings configured here.
<b>Server Name</b>	Specifies the host where the target syslog process is running.

Feature	Description
<b>Server port</b>	Specifies the port where the target syslog process is listening.
<b>Facility</b>	Specifies the designated syslog facility to use for all outgoing messages. Possible values are KERN, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR, NEWS, UUCP, CRON, AUTHPRIV, FTP, LOCAL1 through LOCAL7.
<b>Encoding</b>	Specifies the encoding to use for text in syslog messages, for example, UTF-8.
<b>Format</b>	Specifies the message format. Possible values are: Default, PCI DSS, or SEC.
<b>Protocol</b>	Specifies the communications protocol used when sending syslogs: UDP or TCP. By default, the UDP protocol is selected.
<b>Max length</b>	Specifies the maximum length in bytes of any syslog message. The default value is <b>2048</b> . Messages that exceed the maximum length are truncated when the <b>Truncate overly large syslog messages</b> checkbox is selected.
<b>Truncate overly large syslog messages</b>	When checked, any messages exceeding the maximum length are truncated.
<b>Include the local timestamp in syslog messages</b>	When checked, NetWitness Suite includes the local timestamp in messages.
<b>Include the local hostname in syslog messages</b>	When checked, NetWitness Suite includes the local hostname in syslog messages.
<b>Optionally use IDENT protocol</b>	When checked, NetWitness Suite prepends the identity string to outgoing syslog alerts.



Feature	Description
<b>Identity string</b>	This is an identity string to be prepended to each syslog alert. If the string is blank, no identity string is prepended to the outgoing syslog alerts. You can use this to identify the source of the alert. Users conventionally set it to the name of the program that sends the syslog message.
<b>Apply</b>	Applies the syslog configuration settings.

## SNMP Settings

The following table describes the available options for configuring SNMP notifications for Entitlement, legacy Event Source Management (ESM), Warehouse Connector monitoring, and Archiver monitoring.

Feature	Description
<b>Enable</b>	Enables the SNMP settings configured here.
<b>Server Name</b>	Specifies the SNMP trap host.
<b>Server port</b>	Specifies the listening port on the SNMP trap host
<b>SNMP version</b>	Specifies the SNMP version, <b>v1</b> or <b>v2c</b> .
<b>Trap OID</b>	Specifies the object ID for the SNMP trap on the trap host that receives the audit event. The default value is <b>0.0.0.0.1</b> .
<b>Community</b>	Specifies the community string used to authenticate on the SNMP trap host, the default value is <b>public</b> .
<b>Enable</b>	Enables SNMP notifications as configured here.
<b>Apply</b>	Applies the SNMP configuration settings.

## Supported CEF Meta Keys

This topic describes the Common Event Format (CEF) meta keys that NetWitness Suite global audit logging supports.

Global audit logging templates that you define for a Log Decoder use Common Event Format (CEF) and must meet the following specific standard requirements:

- Include the CEF headers in the template.
- Use only the extensions and custom extensions in a (Key=Value) format from the meta key table below.
- Ensure that the extensions and custom extensions are in the `key=${string}<space>key=${string}` format.

For third-party syslog servers, you can define your own format (CEF or non-CEF).

Procedures related to this table are described in [Define a Template for Global Audit Logging](#) and [Configure Global Audit Logging](#).

## Supported Common Event Format (CEF) Meta Keys

The following table describes the CEF Syslog meta keys that NetWitness Suite global audit logging supports. The Datetime and Hostname fields in the Syslog Prefix are not configurable and not included in the template, but they are prepended to every log message by default. The CEF Header is required to conform to the CEF standard and for any CEF parser. The Extensions and Custom Extensions are optional. The Default Audit CEF Template contains many of the fields in this table. You can add any of the Extensions and Custom Extensions listed to the global audit logging template that you define.

CEF Field	String	Description	NW Meta Keys	Index in Log Decoder
<b>Syslog Prefix</b>				
Datetime	Not Configurable	Syslog Header date time	event.time.s tr	Transient
Hostname	Not Configurable	Syslog Header hostname	alias.host	None

CEF Field	String	Description	NW Meta Keys	Index in Log Decoder
<b>CEF Header</b>		The CEF Header fields are required to conform to the CEF standard and for any CEF parser.		
CEF:Version	CEF:0	CEF Header	--STATIC--	N/A
DeviceVendor	\${deviceVendor}	The product vendor, RSA	-	N/A
DeviceProduct	\${deviceProduct}	The product family. This is always NetWitness Suite Audit.	product	Transient
DeviceVersion	\${deviceVersion}	Host/Service version	version	Transient
Signature ID	\${category}	Identifier of the audit event. It specifies the the category of the audit event.	event.type	None
Name	\${operation}	Description of the event	event.desc	None
Severity	\${severity}	Severity of the audit event	severity	Transient
<b>Extensions</b>				

CEF Field	String	Description	NW Meta Keys	Index in Log Decoder
deviceExternalId	`\${deviceExternalId}`	Unique ID of the host or service generating the audit event	hardware.id	Transient
deviceFacility	`\${deviceFacility}`	Syslog facility used when writing the event to syslog daemon. For example, authpriv.	cs.devfacility	Custom
deviceProcessName	`\${deviceProcessName}`	Name of the executable corresponding to dvcpid	process	None
dpt	`\${destinationPort}`	Destination Port	ip.dstport	None
dst	`\${destinationAddresses}`	Destination IP Address	ip.dst	None
dvcpid	`\${deviceProcessId}`	ID of the process generating the event, which is the process ID of the NetWitness Suite service	process.id	Transient

CEF Field	String	Description	NW Meta Keys	Index in Log Decoder
msg	\${text}	Free text, extra information, or actual description for the event	msg	Transient
outcome	\${outcome}	Outcome of the operation performed corresponding to the audit event	result	Transient
proto	\${transportProtocol}	Network protocol used	protocol	Transient
requestClientApplication	\${userAgent}	Browser detail of the user accessing the page	user.agent	Transient
rt	\${timestamp}	Time at which the event is reported	event.time	None
sourceServiceName	\${sourceService}	The service that is responsible for generating this event	service.name	Transient
spt	\${sourcePort}	Source Port	ip.srcport	Transient

CEF Field	String	Description	NW Meta Keys	Index in Log Decoder
spriv	\${userRole}	User role permissions assignment. For example: admin.owner, appliance.manage,  connections.manage, everyone, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage	privilege	Transient
src	\${sourceAddress}	Source IP Address	ip.src	None
suser	\${identity}	Identity of the logged on user responsible for generating the audit event	user.dst	None
<b>Custom Extensions</b>				
deviceService	\${deviceService}	Service responsible for generating the event	cs.devservice	Custom

CEF Field	String	Description	NW Meta Keys	Index in Log Decoder
parameters	<code>\${parameters}</code>	API and Operation parameters, which capture specific parameters about a query	index	Transient
paramKey	<code>\${key}</code>	A configuration item key. It is the config param for which the audit event is captured.  For example: <code>/sys/config/stat.interval</code>	cs.key	Custom
paramValue	<code>\${value}</code>	A configuration value. It is the value captured during the update.	cs.value	Custom

CEF Field	String	Description	NW Meta Keys	Index in Log Decoder
userGroup	<code>\${userGroup}</code>	Role assignment. For example: Administrators, Analysts, MalwareAnalysts, Malware_Analysts, Operators, PRIVILEGED_ CONNECTION_ AUTHORITY, SOC_Managers	group	None
referrerURL	<code>\${referrerUrl}</code>	The parent URL that refers to the current URL	url	Transient
sessionId	<code>\${sessionId}</code>	Session or connection identifier	log.session. id	Transient

**Note:** Use all of the extensions in the following format:

```
deviceProcessName=${deviceProcessName} outcome=${outcome}
```

Include a `<space>` between a value and a tagname.

By default, all meta keys are not indexed. In the above table, the **Index in Log Decoder** column shows the state of the `flags` keyword (Transient, None, and Custom). If a key is set to `Transient`, it is parsed but not stored in the database. If it is set to `None`, it is indexed and stored in the database. A key listed as "Custom" does not exist in the `table-map.xml` file and, therefore, it is not stored or parsed at all.

"Maintain the Table Map Files" provides instructions for verifying and updating the table mappings. "Edit a Service Index File" provides information on updating the custom index file on the Concentrator.



## Supported Global Audit Logging Meta Key Variables

This topic describes the meta key variables that NetWitness Suite global audit logging supports.

NetWitness Suite provides predefined global audit logging templates that you can use for your global audit logging configurations. For third-party syslog servers, you can define your own template format (CEF or non-CEF) using supported meta key variables.

Procedures related to this table are described in [Define a Template for Global Audit Logging](#) and [Configure Global Audit Logging](#).

### Supported Global Audit Logging Meta Key Variables

The following table describes the meta key variables that NetWitness Suite global audit logging supports. Use these values to create a custom audit logging template for a third-party syslog server.

Variable	Description
<code>\${category}</code>	Identifier of the audit event. It specifies the the category of the audit event.
<code>\${destinationAddress}</code>	Destination IP Address
<code>\${destinationPort}</code>	Destination Port
<code>\${deviceExternalId}</code>	Unique ID of the service generating the audit event
<code>\${deviceFacility}</code>	Syslog facility used when writing the event to syslog daemon. For example, authpriv.
<code>\${deviceProcessId}</code>	ID of the process generating the event, which is the process ID of the NetWitness Suite service
<code>\${deviceProcessName}</code>	Name of the executable corresponding to dvcpid
<code>\${deviceProduct}</code>	The product family. This is always NetWitness Suite Audit.
<code>\${deviceService}</code>	Service responsible for generating the event
<code>\${deviceVendor}</code>	The product vendor, RSA
<code>\${deviceVersion}</code>	Host/Service version

Variable	Description
<code>\${identity}</code>	Identity of the logged on user responsible for generating the audit event
<code>\${key}</code>	A configuration item key. It is the config param for which the audit event is captured.
<code>\${operation}</code>	Description of the event
<code>\${outcome}</code>	Outcome of the operation performed corresponding to the audit event
<code>\${parameters}</code>	API and Operation parameters, which capture specific parameters about a query
<code>\${referrerUrl}</code>	The parent URL that refers to the current URL
<code>\${sessionId}</code>	Session or connection identifier
<code>\${severity}</code>	Severity of the audit event
<code>\${sourceAddress}</code>	Source IP Address
<code>\${sourcePort}</code>	Source Port
<code>\${sourceService}</code>	The service that is responsible for generating this event
<code>\${text}</code>	Free text, extra information, or actual description for the event
<code>\${timestamp}</code>	Time at which the event is reported
<code>\${transportProtocol}</code>	Network protocol used
<code>\${userAgent}</code>	Browser detail of the user accessing the page
<code>\${userGroup}</code>	Role assignment
<code>\${userRole}</code>	User role permissions assignment
<code>\${value}</code>	A configuration value. It is the value captured during the update

## Global Audit Logging Operation Reference

This topic lists message types being logged by the various NetWitness Suite components. Most messages plainly state the operation being logged; when necessary the meaning of the message is explained.

After you create a global audit logging configuration, audit logs automatically go to the external syslog system in the format specified in the selected audit logging template. The message types being logged by the various NetWitness Suite components are shown in the following tables.

### CARLOS

The following table lists the operations logged by CARLOS.

Serial #	Operation Name	Meaning
1	SetProviderConfiguration	A new notification server (for example, SMTP server) was added or updated
2	SetInstanceConfiguration	A new notification type (for example, email destination) was added or updated
3	SetTemplateDefinition	A new template was added or updated
4	RemoveProviderConfiguration	A notification server was removed
5	RemoveInstanceConfiguration	A notification type was removed
6	RemoveTemplateDefinition	A template definition was removed
7	Commit	A configuration bean change was committed
8	Set	A JMX property value was set via NetWitness Suite Explore view

## ESA

The following table lists the operations logged by the Event Stream Analysis (ESA).

Serial #	Operation Name	Meaning
9	SetSourceRequest	A concentrator was added or updated to ESA as source
10	RemoveSourceRequest	A concentrator was removed from ESA as source
11	SetEplModule	An EPL module was deployed or updated to ESA
12	RemoveEplModule	An EPL module was removed from ESA
13	SetEnrichmentSourceRequest	An ESA enrichment source was added/updated
14	RemoveEnrichmentSourceRequest	An ESA enrichment source was removed
15	SetDatabaseReference	An enrichment database reference was made to ESA
16	UpdateEnrichmentData	Data rows added to an ESA enrichment source
17	SetEnrichmentConnection	A connection was made between an EPL module and an enrichment source
18	RemoveEnrichmentConnection	A connection between an EPL module and an enrichment source was removed
19	DisableTrialModule	ESA Trial rules were disabled

## Investigation

The following table lists the operations logged by Investigations.

Serial #	Operation Name	Meaning
1	VisualizePreferences	Operations related to Informer Visualization Request.
2	ParallelCoordinates	Operations related to Loading of Co-Ordinate View Navigation.
3	TimeLine	Operations related to Loading of Timeline View Navigation.
4	ExteralQuery	Operation when a Direct Query is fired via URL.
5	PrintView	Operations to open Investigation in Print View.
6	submitExtractFiles	Operation to submit a Request to Extract files from Sessions.
7	submitExtractLogs	Operation to submit a Request to Extract Logs from Sessions.
8	submitExtractPcap	Operation to submit a Request to Extract Sessions from Sessions.
9	DataScienceDrill	Operation to investigate from Data Science Report.
10	breadCrumbs	Operation to access the Query Breadcumbs.
11	Create	Operation when a new Investigation Query is being saved as a predicate to be used for URL Integration.

Serial #	Operation Name	Meaning
12	userPredicates	Operation to access Recent Queries of a user.
13	chartDefaultMetas	Operation to access last used Meta for generating Coordinate Chart.
14	defaultDevice	Operation to access the Default Investigation Device.
15	deleteDefaultDevice	Operation to delete the Default Investigation Device.
16	chartPreferences	Operation to edit an Investigation Navigation Chart Parameters such as Height.
17	devicePreferences	Operation to save the preferences about the Investigation Device such as Time Range, Profile, Meta Groups etc.
18	topValues	Operation to get the Top Values for Metas. Normally called from Top Values Dashlet.
19	MetaLanguages	Operation to read the Meta Languages from a Device.
20	MetaGroups	Operations related to Investigation Meta Groups.
21	DefaultMetaKeys	Operations related to Investigation Default Meta Keys.
22	UpdateDefaultMetaKeys	Operations to update Investigation Default Meta Keys.

Serial #	Operation Name	Meaning
23	UpdateMetaGroup	Operations to update Investigation Meta Groups.
24	ApplyMetaGroup	Operations to use Investigation Meta Groups.
25	DeactivateMetaGroup	Operations to reset Investigation Meta Groups in UI.
26	DeleteMetaGroup	Operations to remove Investigation Meta Group.
27	DeleteMetaGroups	Operations to remove multiple Investigation Meta Groups.
28	ImportMetaGroups	Operations to import Investigation Meta Groups.
29	ExportMetaGroup	Operations to export multiple Investigation Meta Groups.
30	GeoMap	Operation to access the Geo Map View of Investigation.
31	deleteEndpointCache	Operation to clear Reconstruction Cache of a Device.
32	delete	Operation to delete Alert Templates.
33	CustomColumnGroup	Operation to apply or read Custom Column Group.
34	Import	Operations related to Import of Column Group or Profiles.
35	Export	Operations related to Export of Column Group or Profiles.

Serial #	Operation Name	Meaning
36	SaveProfile	Operation to save an Investigation Profile.
37	ApplyProfile	Operation to apply an Investigation Profile.
38	DeactivateProfile	Operation to deactivate an Investigation Profile.
39	DeleteProfile	Operation to delete an Investigation Profile.
40	DeleteProfiles	Operation to delete multiple Investigation Profiles.

## Reporting Engine

The following table lists the operations logged by the Reporting Engine.

Serial #	Operation Name	Meaning
1	TEMPLATE	For all operations related to template
2	CHART	For all operations related to chart
3	REPORT	For all operations related to report
4	RULE	For all operations related to rule
5	IMAGE	For all operations related to Logo Images used in Reports.
6	LIST	For all operations related to list
7	ALERT	For all operations related to alert
8	CONFIG	For all operations related to configuration change



Serial #	Operation Name	Meaning
9	SCHEDULE	For all operations related to schedule
10	ROLE	For all operations related to role/authorization
11	BATCH_JOB	For all operations related to batch jobs
12	SCHEDULER	For all operations related to scheduler
13	QUERYPROCESSOR	For all operations related to queryprocessor
14	FORMATTER	For all operations related to formatter
15	OUTPUTACTION	For all operations related to outputaction
16	STATUSMANAGER	For all operations related to statusmanager
17	BATCH_RUNDEF	For all operations related to batch rundef
18	CHARTGROUP	For all operations related to chart group
19	REPORTGROUP	For all operations related to report group
20	RULEGROUP	For all operations related to rule group
21	LISTGROUP	For all operations related to list group
22	DISKSPACE	For all operations related to disk space

## Warehouse Connector

The following table lists the operations logged by the Warehouse Connector.

Serial #	Operation Name	Meaning
1	LockBox Password Create	Operation to create LockBox Password.
2	LockBox Password Update	Operation to update LockBox Password.
3	LockBox Password Refresh	Operation to refresh LockBox Password.
4	Adding Stream	Operation to add a Stream.
5	Adding Source	Operation to add a Source.
6	Adding Destination	Operation to add a Destination.
7	Removing	Operation to remove a Source, Stream, or Destination.
8	Changing Password	Operation to change the Password.
9	Updating Source	Operation to update a Source.
10	Adding Source to Stream	Operation to add a Source to a Stream.
11	Deleting Source from Stream	Operation to delete a Source from a Stream.
12	Setting Destination to Stream	Operation to set a Destination to a Stream.
13	Finalizing Stream	Operation to finalize a Stream and initiate the aggregation.
14	Stopping Stream	Operation to stop a Stream.

Serial #	Operation Name	Meaning
15	Starting Stream	Operation to start a Stream.
16	Reloading Stream	Operation to reload a Stream.

## Health & Wellness

The following table lists the operations logged by Health & Wellness.

Serial #	Operation Name	Meaning
1	SavePolicyRequest	Operation while adding or modifying a Policy.
2	RemovePolicyRequest	Operation while removing a Policy.

## NetWitness Suite Core Services

The following table lists the operations logged by NetWitness Suite Core Services.

Serial #	Operation Name	Meaning
1	FILE-Command	Operation to list, retrieve and delete files from approved directories on this device.
2	SERVICE-Start	Service started
3	SERVICE-Stop	Service stopped
4	REDIRECT-Syslog	Operation for syslog forwarding.
5	ADD-Monitor	Issuing a filesystem monitor operation
6	DELETE-Monitor	Issuing a filesystem monitor deletion operation
7	SHUTDOWN-Service/shutdown.service	Shutting down appliance service
8	REBOOT-Service	Restarting appliance service

Serial #	Operation Name	Meaning
9	CONFIGURE-Network	Issuing Network Configuration change
10	SET-NTP	Issuing NTP set operation
11	STOP-NTP	Issuing NTP stop operation
12	NTP-Timesync	Issuing NTP time sync operation
13	SET-SNMP	Issuing SNMP set
14	UPGRADE/upgrade	Issuing upgrade operation
15	create.collection	Operation to create an empty collection.
16	restore	Issuing restore
17	session.aggregation	Issuing aggregation start/stop
18	add.device	Adding a device for aggregation
19	edit.device	Editing a device used for aggregation
20	delete.device	Deleting a device used for aggregation
21	capture.start	Starting capture operation
22	capture.stop	Stopping capture operation
23	select.interface	Selecting capture interface
24	export	Operation to export packets or sessions.
25	reload	Issuing a parser reload
26	schema	Issuing a schema request for loaded parsers
27	upload/file.upload	Issuing file upload

Serial #	Operation Name	Meaning
28	notify	Issuing feed notify
29	delete	Issuing file deletion
30	edit.config	Configuration change operation
31	parsers.transforms	Perform a language key transformation
32	data.reset	Data reset operation
33	timeout	REST request timeout
34	cancel	Cancel a running query
35	timeroll	Operation to delete the database files that exceed a given limit.
36	dump	Operation to dump information out of the database in nwd formatted files.
37	session.wipe	Issuing a session wipe operation
38	REPLACE-Rule	Issuing a rule replace operation
39	MERGE-Rule	Issuing a rule merge operation
40	ERASE-Rule	Issuing deletion of a set of all rules
41	ADD-Rule	Issuing a rule addition operation
42	DELETE-Rule	Issuing deletion of a set of rules
43	sdk.info	Issuing SDK summary info.
44	sdk.session	Issuing SDK session info.
45	sdk.language	Issuing SDK language
46	sdk.aliases	Issuing SDK alias request

Serial #	Operation Name	Meaning
47	sdk.transform	Issuing SDK transformation request
48	sdk.search	Issuing session content search request
49	sdk.cache	Operation related to session content cache
50	sdk.content	Issuing session content request
51	check.authorization	Operation to check user roles for permissions to execute an operation.
52	close.connection	Issuing a connection close operation
53	handshake	Issuing an SSL handshake
54	logon/login	Operation to login from NW to the other services, mostly to privileged users.
55	STOREDPROCOP	Issuing file upload cancel/start
56	ADD-Task	Added scheduled task
57	DELETE-Task	Deleted scheduled task
58	logoff	Issuing logout operation
59	list.cacerts	Issuing list trusted CA certificate operation
60	delete.cacerts	Issuing delete trusted CA certificate operation
61	add.cacerts	Issuing addition of trusted CA certificate operation
62	restart.command	Issuing restart command line option

Serial #	Operation Name	Meaning
63	delete.file/file.delete	Operation to delete system configuration files.
64	update.file/file.update	Operation to update system configuration file.
65	create.file	Issuing file creation operation
66	query	Issue a database query
67	unlock	Issuing unlock user account operation
68	user.add	Operation to create user accounts on individual devices.
69	user.delete	Operation to delete a user on individual devices.
70	group.create	Operation to add a new group to the system.
71	user.remove	Remove a user account from a group
72	group.delete	Delete a group from the /users/groups tree
73	add.user	Issuing add user command to collection
74	delete.user	Issuing delete user command to collection
75	remove.user	Removing an user from collection
76	collection.open	Issuing an open command for a collection

Serial #	Operation Name	Meaning
77	collection.close	Issuing a close command for a collection
78	collection.delete	Issuing collection deletion command
79	reingest.start	Operation to start reingesting of packet data in collection.
80	feed.notify	Issuing a feed notify command
81	collect	Issuing a collect command
82	collect.start	Issuing a data collection start
83	collection.global	Issuing import parser command
84	parser.reload	Issuing parser reload command
85	reingest	Operation to reingest packet data in collection.
86	collection.create	Issuing a create collection command
87	collection.restore	Issuing a restore collection command
88	collection.clone	Issuing a clone collection command
89	parser.reload	Issuing parser reload command
90	sdk.query	Performs a query against the meta database
91	sdk.msearch	Search for pattern matches in many sessions or packets
92	sdk.values	Performs a value count query and returns the matching values for a report



Serial #	Operation Name	Meaning
93	sdk.timeline	Returns the count of sessions/size/packets in discrete time intervals

## Malware Analysis

The following table lists the operations logged by the Malware Analysis (MA) component.

Serial #	Operation Name	Meaning
1	GetDashBoardSummaryRequest	Get dashboard analysis statistics
2	GetFileScoreSummaryRequest	Get aggregated file scores by score type and risk level
3	CountEventsAndFilesRequest	Get count of events and files over a time frame
4	GetAvVendorDetectionRequest	Get AV vendor analysis results
5	GetAVVendorsRequest	Get list of AV Vendors supported
6	SetInstalledAVVendors	Request Update list of installed AV Vendors in config
7	CountEventByCriteriaRequest	Count events by criteria
8	FindEventByIdRequest	Get event by id
9	FindEventByCriteriaRequest	Get event by criteria
10	DeleteEventRequest	Delete event
11	CommentOnEventRequest	Add comment to event
12	ReSubmitEventRequest	Resubmit event for analysis
13	FindEventScoreByIdRequest	Get event score by event id

Serial #	Operation Name	Meaning
14	FindEventScoreByCriteriaRequest	Get event score by criteria
15	FindMetaByIdRequest	Get meta by id
16	FindMetaByCriteriaRequest	Get meta by criteria
17	FindMetaValueByCriteriaRequest	Get meta value by criteria
18	CountByDistinctMetaValueRequest	Count distinct meta values
19	CountByMetaNameAndValueWithDateRangeIntervalRequest	Count meta and values with interval for charting
20	CountByValueAndAverageOverallScoreRequest	Count meta and map to overall scores for events
21	CountByValueAndAverageGroupScoreRequest	Count meta and map to group scores for events
22	CountFileEntryByCriteriaRequest	Count files by criteria
23	FindFileEntryByIdRequest	Get file by id
24	FindFileEntryByCriteriaRequest	Get file by criteria
25	ReSubmitFileEntryRequest	Resubmit file for analysis
26	FileDownloadRequest	Download file from repository
27	FileUploadRequest	Upload file for analysis
28	FindFileScoreByIdRequest	Get file score by id
29	FindFileScoreByCriteriaRequest	Get file score by criteria
30	FindHashValueByIdRequest	Get whitelist/blacklist Hash value by id
31	FindHashValueByCriteriaRequest	Get whitelist/blacklist Hash value by criteria
32	AddHashValueRequest	Add whitelist/blacklist Hash value

Serial #	Operation Name	Meaning
33	UpdateHashValueRequest	Update whitelist/blacklist Hash value
34	DeleteHashValueRequest	Delete whitelist/blacklist Hash value
35	FindHashValueByMd5Request	Find whitelist/blacklist Hash value by md5
36	AddHashValueInFileRequest	Add File to repository as well as hash value
37	GetDefaultRulesRequest	Get default IOC Rules configuration
38	ResetToDefaultRulesRequest	Reset IOC Rules configuration to default
39	GetAllOverrideRulesRequest	Get IOC Rules user created override configuration
40	FindOverrideRuleByIdRequest	Find IOC override rule by id
41	AddOverrideRuleRequest	Add IOC override rule
42	UpdateOverrideRuleRequest	Update IOC override rule
43	DeleteOverrideRuleRequest	Delete IOC override rule
44	SubmitOnDemandNextGenRequest	Submit new ondemand nextgen scan
45	FindOnDemandJobEntryByIdRequest	Get ondemand job entity by id
46	FindOnDemandJobEntryByCriteria Request	Get ondemand job entity by criteria
47	GetOnDemandJobInfoRequest	Get ondemand job reference entity by id
48	GetOnDemandDefaultConfiguration	Request Get ondemand default configuration

Serial #	Operation Name	Meaning
49	CancelOnDemandJobRequest	Cancel ondemand job in progress
50	DeleteOnDemandJobRequest	Delete ondemand job
51	ReSubmitOnDemandJobRequest	Resubmit ondemand job
52	SubscriptionRequest	Subscribe to MA Cloud communication
53	UnSubscribeRequest	Unsubscribe from MA Cloud communication
54	GetTopEventInfluencesRequest	Get Top N event influences
55	GetServerInfoRequest	Get server info, such as server time
56	DataResetRequest	Reset database
57	OnDemandJobStatusNotification	Report ondemandjob progress to subscribers
58	LicenseStatusNotification	Report license status - num samples analyzed
59	DataResetNotification	Report that data was reset
60	GetIocSummaryRequest	Get IOC rules aggregated by event/file scores
61	FindAlertTemplatesByCriteriaRequest	Get rabbitmq alert templates by criteria
62	SaveAlertTemplateRequest	Update alert template
63	DeleteAlertTemplateRequest	Delete alert template
64	GetJobStatusRequest	Get in progress job analysis thread status
65	GetEventTypeCountSummaryRequest	Get event analysis counts by date chart

Serial #	Operation Name	Meaning
66	Logon	Logon to the MA Service
67	Modified	Modifying config changes
68	GetNextGenSummaryRequest	Get nextgen dashboard summary statistics

### NetWitness Suite User Interface

The following table lists the operations logged by the NetWitness Suite User Interface component.

Serial #	Operation Name	Meaning
1	uploadTrialLicense	Upload Trial License
2	LicenseEntitle	Entitle License
3	LicenseDeactivation	Deactivate License
4	ExpiredLicense	License Expired
5	LicenseOutOfComplianceAcknowledgement	EULA Acknowledgement
6	resetLicense	Reset License
7	usageDateExport	License data usage - csv/pdf
8	refreshLicense	Refresh LLS license
9	LicenseOutOfCompliance	Out of Compliance
10	OOTBEntitlementOutOfCompliance	OOTB Trial license Out of Compliance
11	OOTBEntitlementFirstLoginTimeModified	OOTB time modified
12	OOTBEntitlementFileDeleted	OOTB File deleted
13	OOTBEntitlementDataTampering	OOTB data tampering

Serial #	Operation Name	Meaning
14	uploadOfflineResponse	Upload offline response
15	offlineDownloadCapRequest	Download offline request
16	movePerpetualToMetered	Move Service-based license to Metered
17	moveMeteredToPerpetual	Mover Metered to Service-based license
18	mapServiceLicense	Map Service to Real license
19	delete	Operation to delete Alert Templates.
20	HttpRequest	Operation for Audit Logging of the accessed URL.
21	Page Accessed	Operation for Audit Logging of the accessed page.
22	Navigate	Operation to navigate to the accessed page.
23	Events	Operation to view the accessed event page.
24	Recon	Operation for Event Reconstruction requested.
25	Services	Operation while reading the list of available devices for investigation.
26	Service	Operation for a List of devices requested to be investigated.

Serial #	Operation Name	Meaning
27	Collections	Operation to view the list of collections requested.
28	Profiles	Operation to apply a Profile.
29	ColumnGroups	Operation to apply or read Column Group.
30	ParallelCoordinates	Operations related to Loading of co-ordinate view navigation.
31	Timeline	Operations related to loading of timeline view navigation.
32	PrintView	Operations to open investigation in print view.
33	Preferences	Operations related to Informer Request.
34	import	Operations related to Import of Column Group or Profiles.
35	export	Operations related to Export of Column Group or Profiles.
36	Predicate	Operations related to Queries (Predicates) used for Investigation.
37	Languages	Operation for Language requested from a Device.
38	CancelLanguageLoad	Operation for Language Load Canceled from Navigate Page.

Serial #	Operation Name	Meaning
39	summary	Operation for a summary requested from a Device.
40	languages	Operation for a language requested from a device.
41	aliases	Operation for meta aliases requested from a device.
42	query	Operation for SDK Query requested from a device.
43	msearch	Operation for a meta search requested from a device.
44	nodeListing	Node Listing for a node requested from a Device.
45	content	SDK Content call requested from a Device for downloading a PCAP or Log.
46	Export Files	File Listing Requested for a Session in File View or Extraction jobs.
47	packets	Packets requested for sessions in Packet View or Extraction Jobs.
48	deleteEndpointCache	Operation to clear reconstruction cache of a device.



Serial #	Operation Name	Meaning
49	Logon	Operation for user to sign in to NetWitness Suite User Interface.
50	Logoff	Operation for user to sign out of NetWitness Suite User Interface.
51	defaultDevice	Operation to access the Default SA UI Device.
52	deleteDefaultDevice	Operation to delete the Default investigation device.
53	submitExtractFiles	Operation to submit a request to Extract files from Sessions.
54	submitExtractLogs	Operation to submit a Request to Extract Logs from Sessions.
55	submitExtractPcap	Operation to submit a Request to Extract Sessions from Sessions.
56	MetaGroup	Operations related to SA UI Meta Groups.
57	ExternalQuery	Operation when a Direct Query is fired via URL.
58	GeoMap	Operation to access the Geo Map View of Investigation.
59	SaveProfile	Operation to save an Investigation Profile.

Serial #	Operation Name	Meaning
60	ApplyProfile	Operation to apply an Investigation Profile.
61	DeleteProfile	Operation to apply an Investigation Profile.
62	DeactivateProfile	Operation to apply an Investigation Profile.
63	VisualizePreferences	Operations related to Informer Visualization Request.
64	ExportMetaGroup	Operations to export multiple SA UI Meta Groups.
65	userPredicates	Operations to export multiple SA UI Meta Groups.
66	FileView	Operation for reconstruction request for File View.
67	resource.update	Operation when Live Subscription State changes.

## Respond

The following table lists the operations logged by the RESPOND component.

Serial #	Operation Name	Meaning
1	update	Update notification setting
2	update	Update integration settings configuration
3	delete	Delete Alerts
4	create	Create new incident

Serial #	Operation Name	Meaning
5	update	Update incident details
6	read	Read incident details
7	delete	Delete incidents
8	read	Read remediation tasks
9	delete	Delete Remediation tasks
10	update	Update remediation tasks
11	create	Create new rule
12	update	Update existing alert rule
13	reorder	Reorder priority of alert rules

## Local Audit Log Locations

NetWitness Suite has global audit logging capabilities. When you configure global audit logging, audit logs from all NetWitness Suite components collect in a centralized system, which converts them into the required format and forwards them to a third-party syslog server or a Log Decoder.

To view audit logs from the individual services, you can look at the local audit log locations. The following table shows the local directory paths of the audit logs for the NetWitness Suite user interface and the various NetWitness Suite services.

Service/Module	Audit Log Location
NetWitness Suite User Interface (NetWitness Suite Web Server)	<p>The NetWitness Suite user interface sends audit logs to the following locations:</p> <ul style="list-style-type: none"> <li>• <b>/var/lib/netwitness/uax/logs/audit/audit.log</b> (human-readable format)</li> <li>• Syslog running on the local host (JSON format)</li> </ul> <p>The NetWitness Suite user interface uses the AUTH facility of syslog to write audit logs to syslog. You can only see audit logs in the first location (<b>/var/lib/netwitness/uax/logs/audit/audit.log</b>).</p>
Core Services (Decoder, Log Decoder, Concentrator, Broker, and Archiver), Log Collector, Warehouse Connector, Workbench, and IPDB Extractor	<p>The Core services and similar services send audit logs to Syslog running on the local host.</p> <p>Path: <b>/var/log/secure</b> (JSON format)</p> <p>The Core services use the AUTHPRIV facility of syslog to write audit logs to syslog.</p>

Service/Module	Audit Log Location
Reporting Engine, Malware Analysis, RESPOND, and Event Stream Analysis (ESA)	<p>These services send audit logs to the following locations:</p> <ul style="list-style-type: none"> <li>• <b>&lt;application home directory&gt;/logs/audit/audit.log</b> (human-readable format)</li> <li>• Syslog running on the local host (JSON format)</li> </ul> <p>The following are the audit log locations of these services:</p> <p>Reporting Engine:  <b>/home/rsasoc/rsa/soc/reporting-engine/logs/audit/audit.log</b></p> <p>Respond Server  <b>/var/log/netwitness/respond-server/respond-server-audit.log</b></p> <p>Malware Analysis:  <b>/var/lib/netwitness/rsamalware/spectrum/logs/audit/audit.log</b></p> <p>Event Stream Analysis:  <b>/opt/rsa/esa/logs/audit/audit.log</b></p> <p>These services use the AUTH facility of syslog to write audit logs to syslog. You can only see audit logs in the first location (&lt;application home directory&gt;/logs/audit/audit.log).</p>
Health & Wellness, Event Source Management (ESM), and Appliance and Service Grouping (ASG)	<p>These Services send audit logs to the following locations:</p> <ul style="list-style-type: none"> <li>• <b>/opt/rsa/sms/logs/audit/audit.log</b> (human-readable format)</li> <li>• Syslog running on the local host (JSON format)</li> </ul> <p>These services use the AUTH facility of syslog to write audit logs to syslog. You can only see audit logs in the first location (/opt/rsa/sms/logs/audit/audit.log).</p>

