NetWitness® Platform

Version 12.4

System Configuration Guide

NETWITNESS

Platform

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by RSA.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

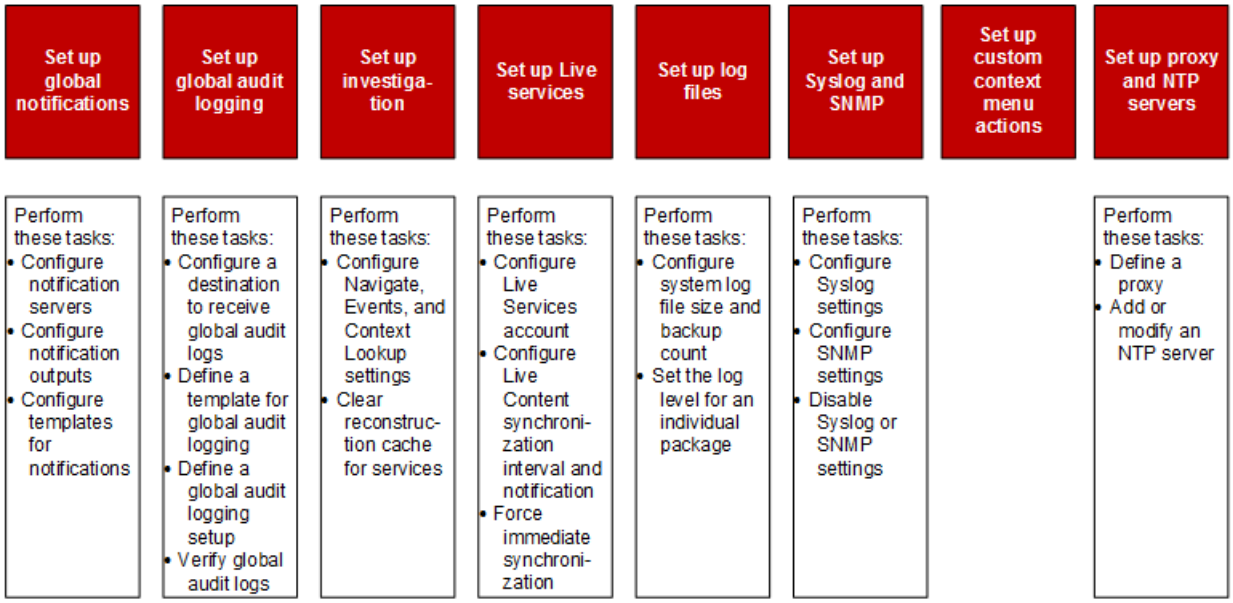
This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

April, 2024

Contents

System Configuration Overview

In the Administration System view, administrators can configure system settings to receive optimal performance from NetWitness. This diagram show 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. 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, 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.
- 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. 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

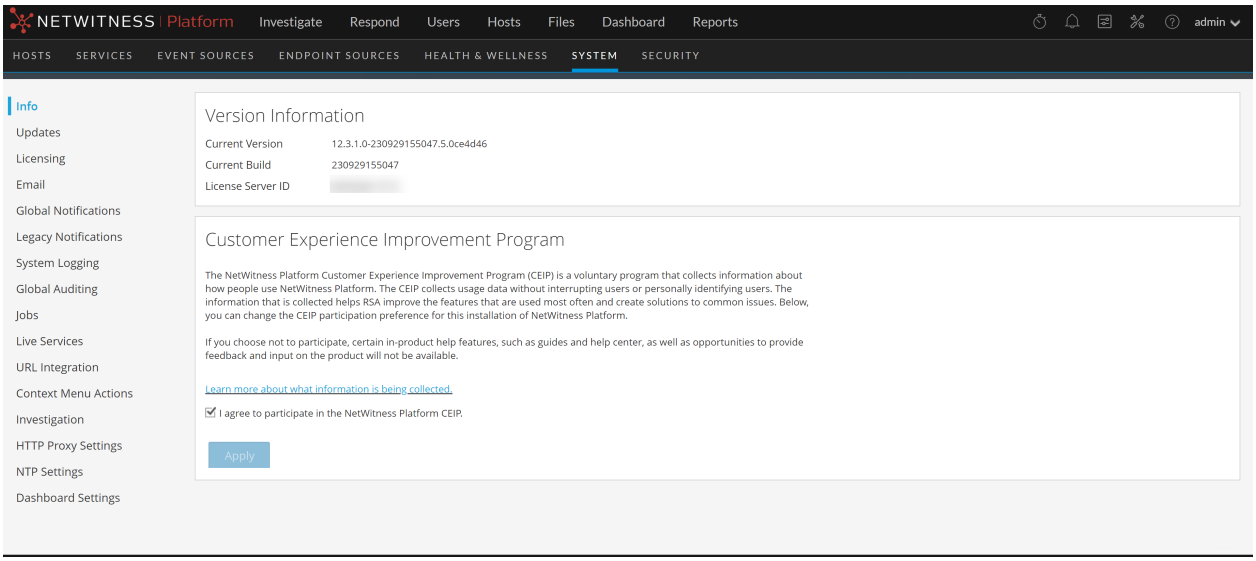
Configure Log File Settings

Access System Settings

This topic introduces the system configuration capabilities of NetWitness 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.

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 the Customer Experience Improvement Program

The NetWitness Platform Customer Experience Improvement Program (CEIP) is an initiative to improve NetWitness Platform continuously. When a customer enables this program, the CEIP performs analytics about how individual users work in NetWitness Platform without interrupting their workflow or personally identifying users. As part of this program, NetWitness gains insights on your deployment and license usage and analytics on pages viewed and actions taken. NetWitness uses these analytics when making decisions about new features and enhancements to prioritize in upcoming releases. For more information, see Customer Experience Improvement Program and Live Feedback: Learn More.

By default, a dialog box is shown to enable or disable the CEIP program if users have not already subscribed to the program. When a user with ***config-server.configuration.manage***, ***Access Live Module***, ***Manage Live System Settings***, and ***Access Administration Module*** permissions login to NetWitness Platform for the first time on a server that did not have NetWitness Live Feedback enabled, a popup dialog presents the option to enable the feature. Users who log in later do not see the dialog, but any Administrator or users with required permissions can disable or enable the feature anytime.

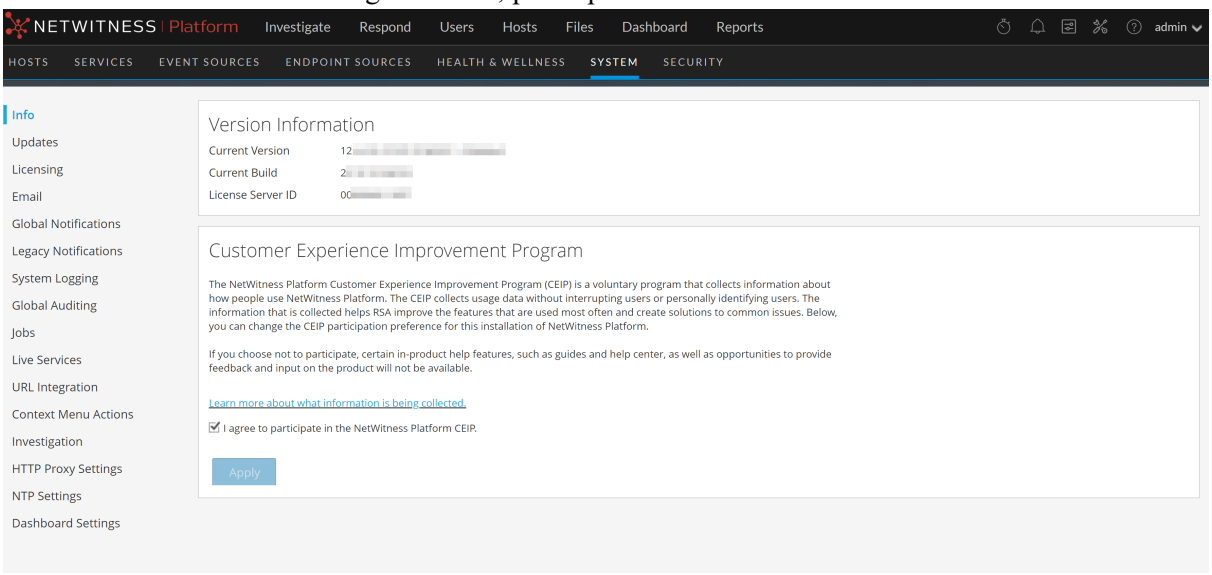
In Version 12.3.1.0 or later, the CEIP program dialog is displayed to all the users who previously did not enable the CEIP program and are upgrading to a major or minor NetWitness Platform version. For example, in NetWitness Platform version 12.3.1.0, the major version is represented by 12 while the minor version is represented by 3.

Disable or Enable Participation in the CEIP

All user roles with permission to view the (Admin) > **System** > **Info** panel can see if the program is enabled or not, but only users with ***config-server.configuration.manage***, ***Access Live Module***, ***Manage Live System Settings***, and ***Access Administration Module*** permissions assigned to their user role can change the setting. The built-in Administrators role has these permissions assigned by default. To view or change permissions assigned to a role, see "Change Permissions Assigned to a Role" in the *System Security and User Configuration Guide*.

To enable or disable participation in the program:

1. As a user with the required permissions, log in to the NetWitness Platform.
2. Go to **(Admin)** > **System** > **Info**.
   The checkbox next to **I agree to participate in the NetWitness Platform CEIP** indicates whether the feature is enabled. In the figure below, participation is enabled.



3. Do one of the following:
   a. To enable participation, under Customer Experience Improvement Program, set the checkbox next to **I agree to participate in the NetWitness Platform CEIP**. A check mark indicates that you are agreeing to participate in the program. Click **Apply.**
      NetWitness Platform begins to collect telemetry on page views and click and focus events.
   b. To disable participation after it has been enabled, under Customer Experience Improvement Program, clear the checkbox next to **I agree to participate in the NetWitness Platform CEIP**. An empty checkbox indicates that you do not wish to participate in the program. The check mark is removed and a message advises that some information may be collected on open user sessions

until those users log out of their sessions. Click **Apply.**
The feature is turned off, and collection ends when all open user sessions are closed.

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, New 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. Individual topics describe the relevant procedures. For more information on ESA alert configuration, see "Notification Methods" in the *Alerting with ESA Correlation Rules User 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** > **Global Notifications** > **Servers** tab).

Global Notifications are used by a variety of components in NetWitness, such as Event Stream Analysis (ESA), Respond, Health and Wellness, New 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.

Note: New Health and Wellness supports only Email and Syslog notifications.

Note: ESA SNMP notifications are not supported for NetWitness 11.3 and later.

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.

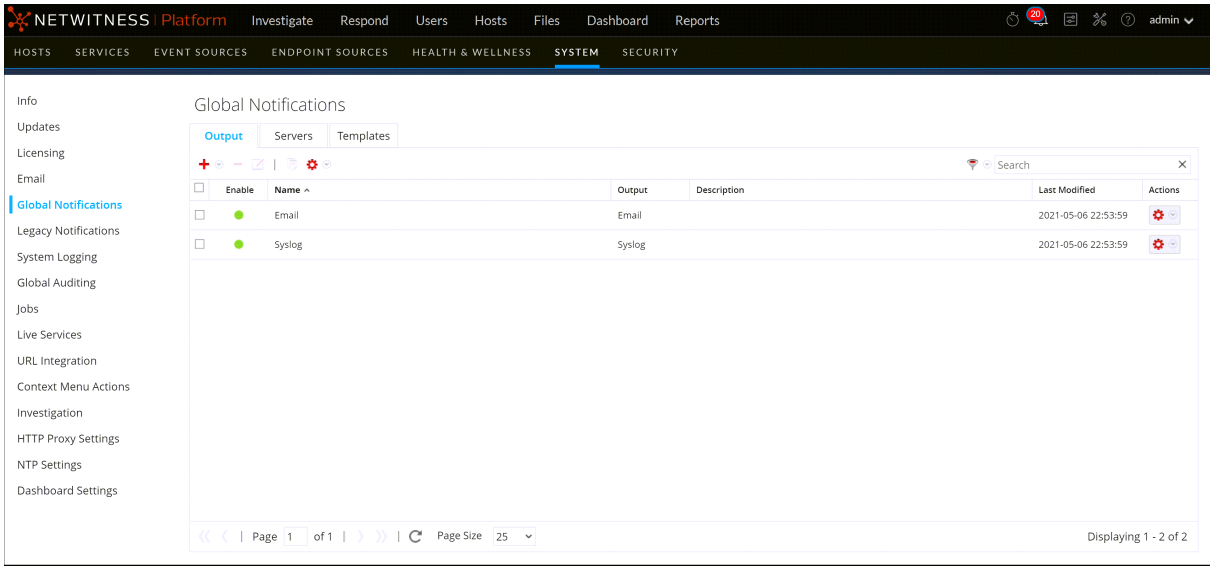
Script notification servers enable you to configure Script as a notification server.

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

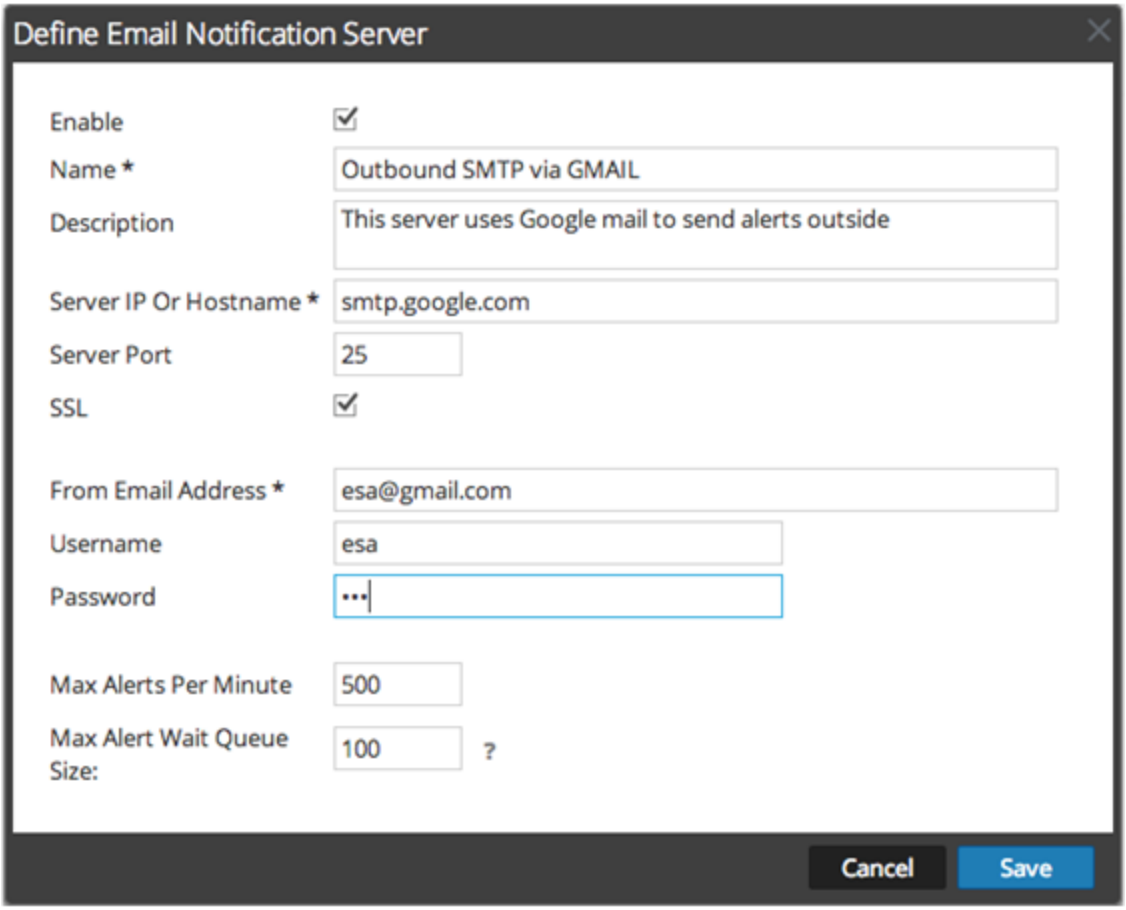
Configure the Email Settings as Notification Server

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.



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



5. 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.

Note:
- If you enable SSL in **Define Email Notification Server** dialog, you must obtain the servers certificate in **.pem** format from the server and then run the following command to install the certificate in the Integration server truststore.

```
security-cli-client --add-trusts -s integration-server -x <mail-server-certificate-filename>.pem -u <username> -k <password>
```

- The preferred Server Port is **587**.

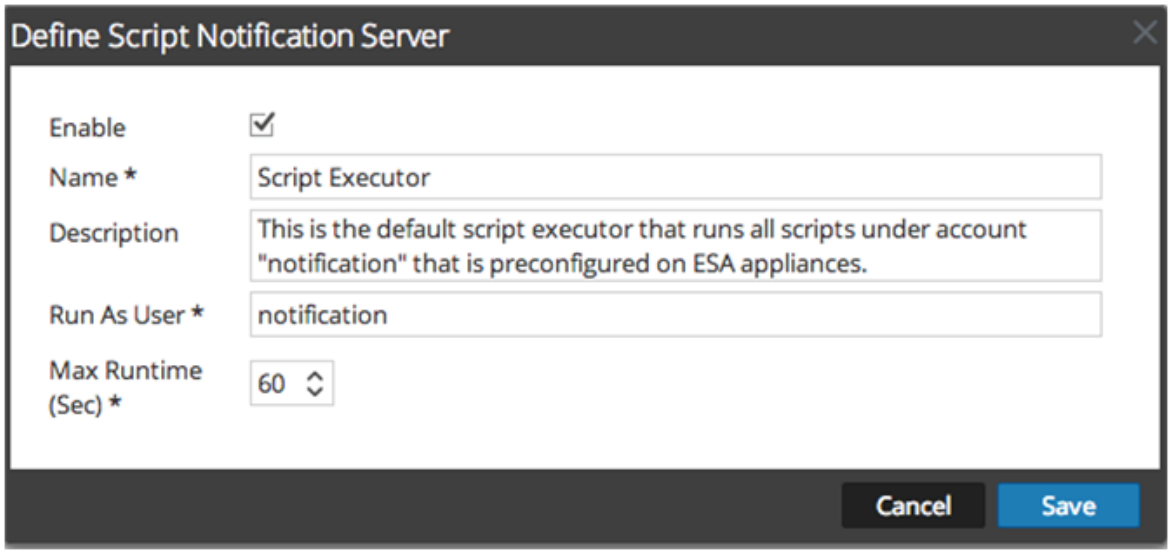
For details of the parameters and descriptions, see Define Notification Server Dialogs

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:

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 **Script**.



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

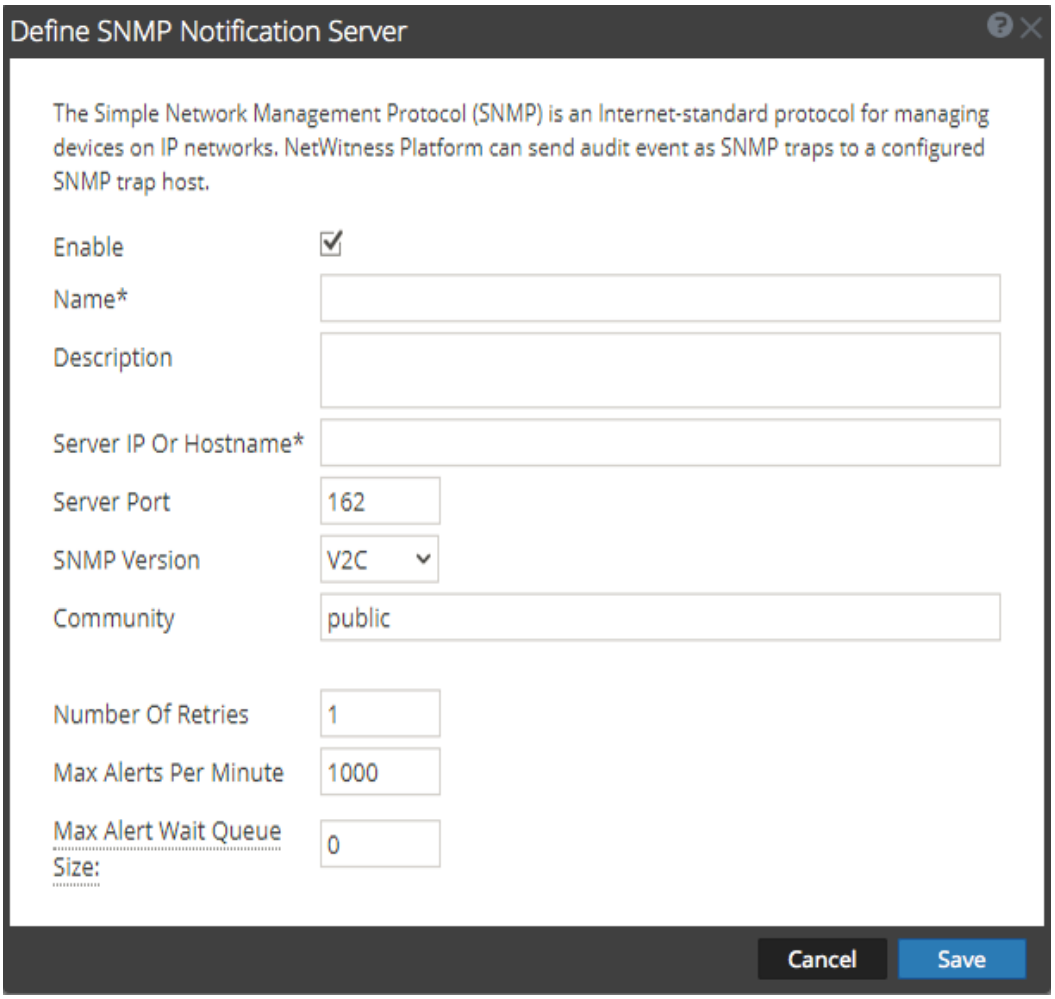
For details of the parameters and descriptions, see Define Notification Server Dialogs.

Configure the SNMP Settings as Notification Server

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

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 **SNMP**.



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.

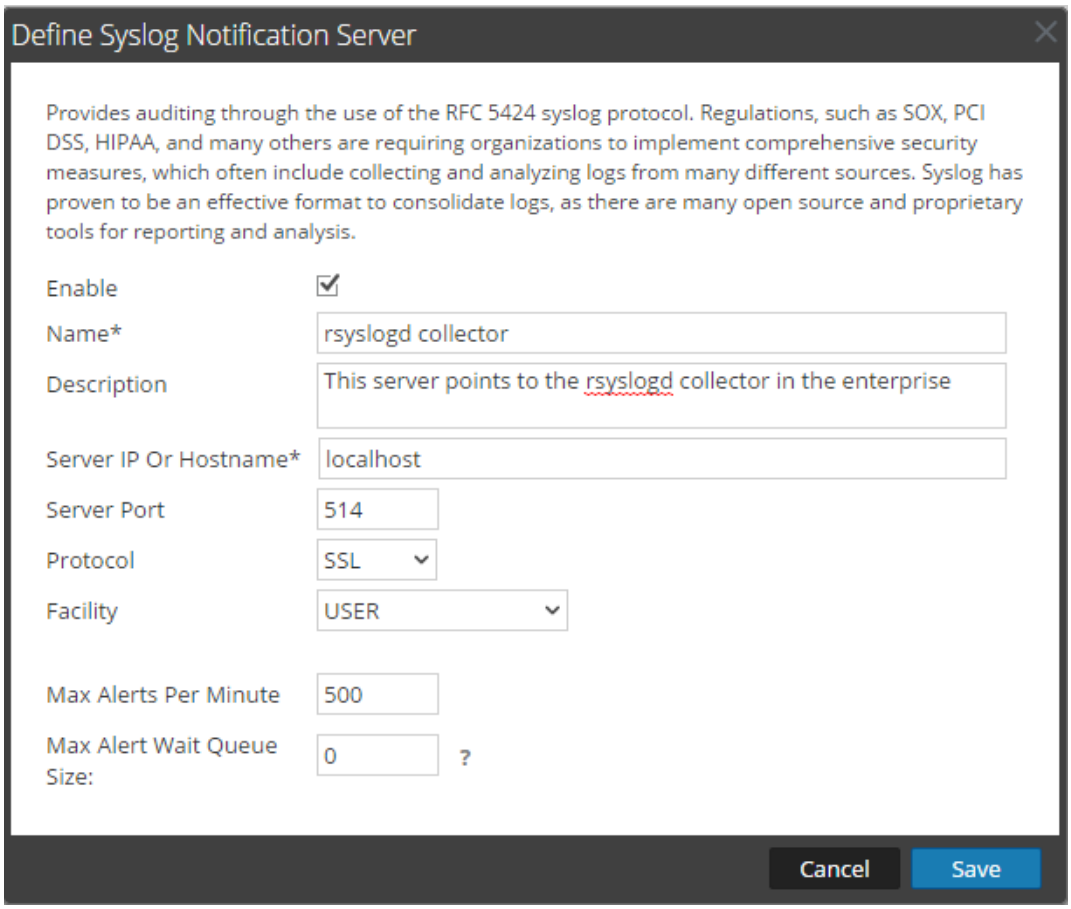
Configure a Syslog Notification Server

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**.



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.

Note: If you select **TCP SSL** as the protocol, you must set the Server Port to **6514** unless any other custom port forwarding mechanism is in place.

Configure Notification Outputs

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

Global Notifications configurations define notifications settings for Event Source Management (ESM), Health and Wellness, New 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. Individual topics describe the relevant procedures. For more information on ESA alert configuration, see "Notification Methods." in the *Alerting with ESA Correlation Rules User Guide*. 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. notification outputs are required when defining an ESA rule. You can configure notification outputs in the Administration System view ((Admin) > **System** > **Global Notifications** > **Output** tab).

Global Notifications configurations define notifications settings for Event Source Management (ESM), Health and Wellness, New 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:

- Email
- SNMP
- Syslog
- Script

Note: New Health and Wellness supports only Email and Syslog notification outputs.

Note: ESA SNMP notifications are not supported for NetWitness 11.3 and later.

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.

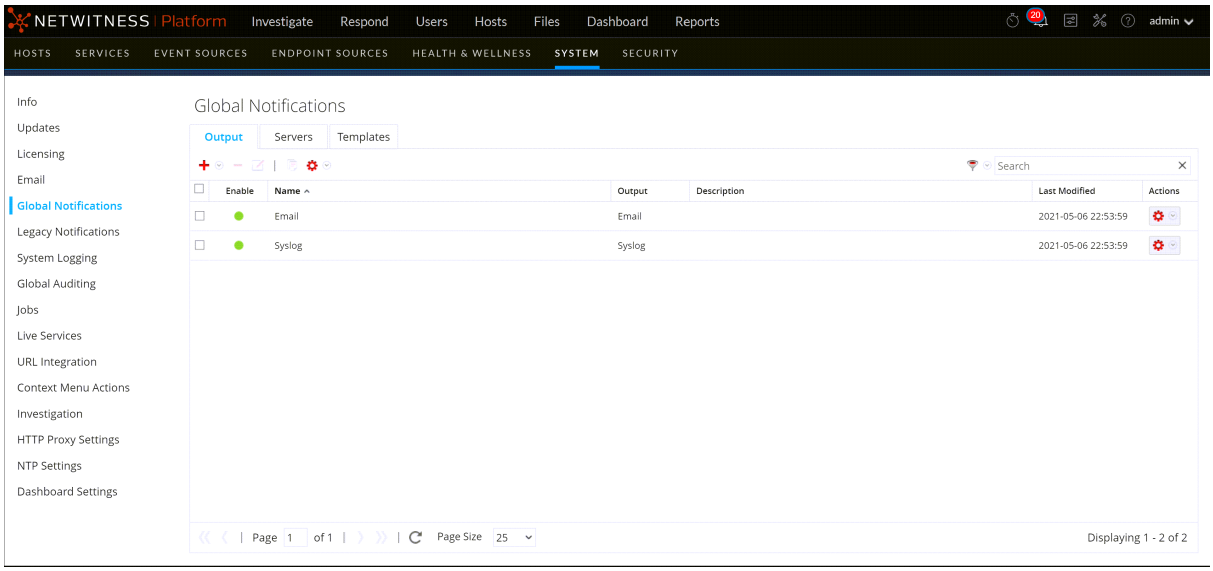
SNMP notification settings enable you to define the SNMP settings to send alert notifications. Syslog notifications enable you to define the Syslog settings used to send alert notifications. Script notifications enable you to define the Script that executes in response to the alert.

For detailed information on the notification configurations, including parameters and descriptions, see Define Notification Server Dialogs.

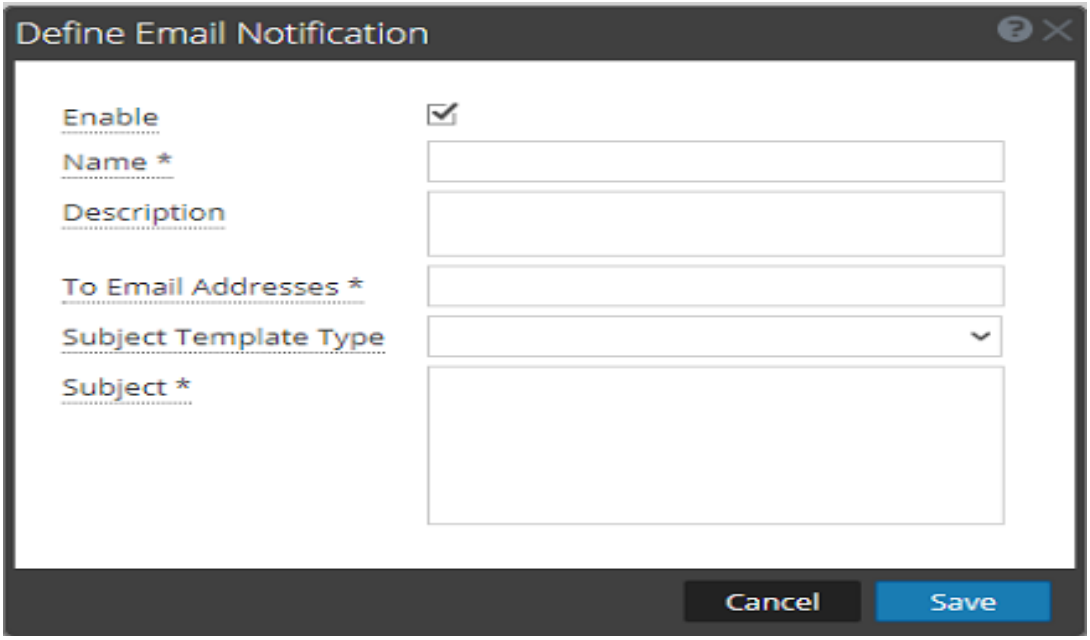
Configure Email as a Notification

To configure Email as a notification:

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



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



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

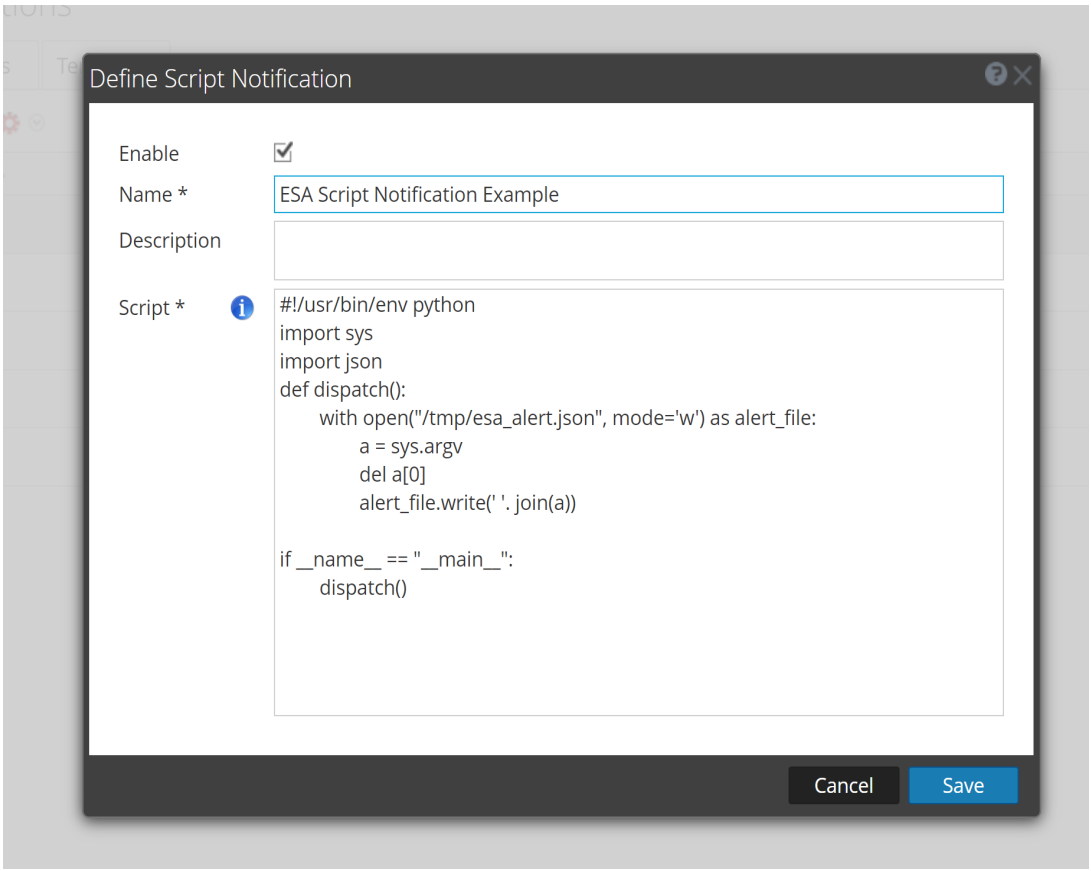
For details of the parameters and descriptions, see Define Notification Server Dialogs.

Configure Script as a Notification

This topic provides instructions to define and configure a Script 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**.
3. On the Output tab, from the  drop-down menu, select **Script**.



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

> **Note:** To retrieve alerts information in the scripts, use command line arguments based on the scripting language. For Example:
> - If you are using Python as the scripting language, use sys.argv (command line arguments) to retrieve alerts information.
> - If you are using Bash as the scripting language, use $*, $1, $2, and $@ (command line arguments) to retrieve alerts information.

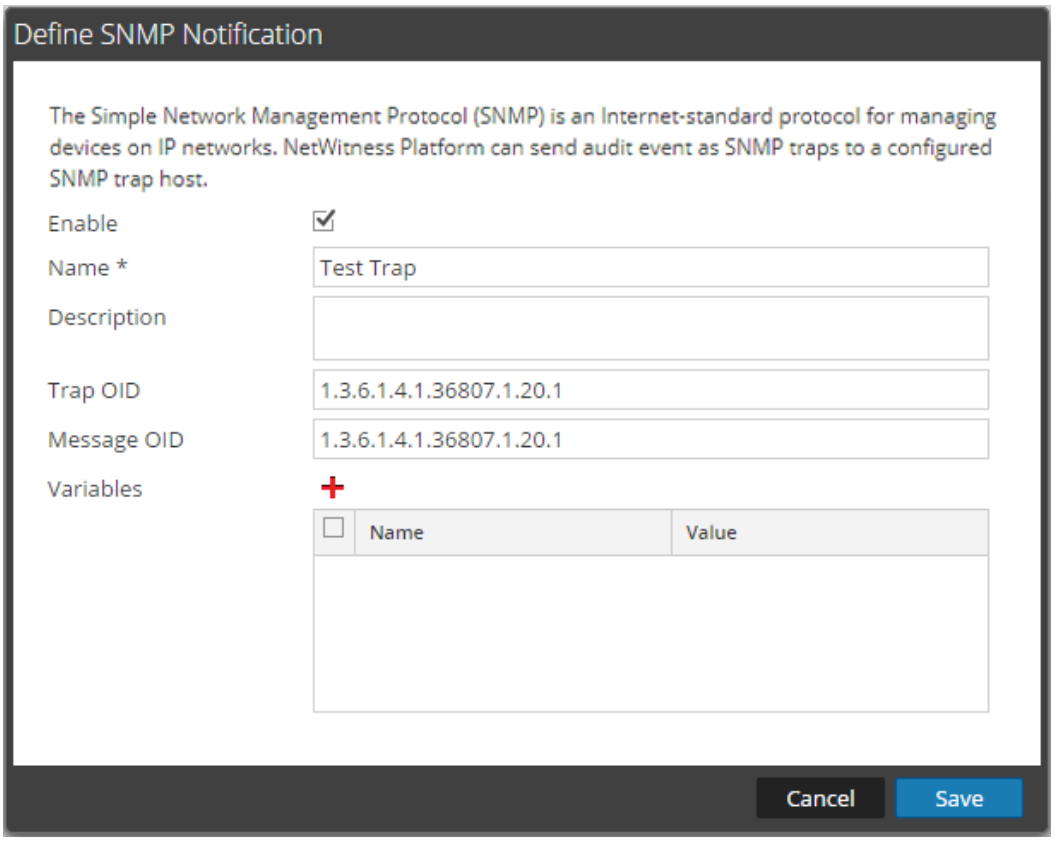
> **Note:** Use **Temp** folder to create files or folders as a part of the script.

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:

1. Go to **(Admin)** > **System**.
2. In the options panel, select **Global Notifications**.
3. On the Output tab, from the drop-down menu, select **SNMP**.



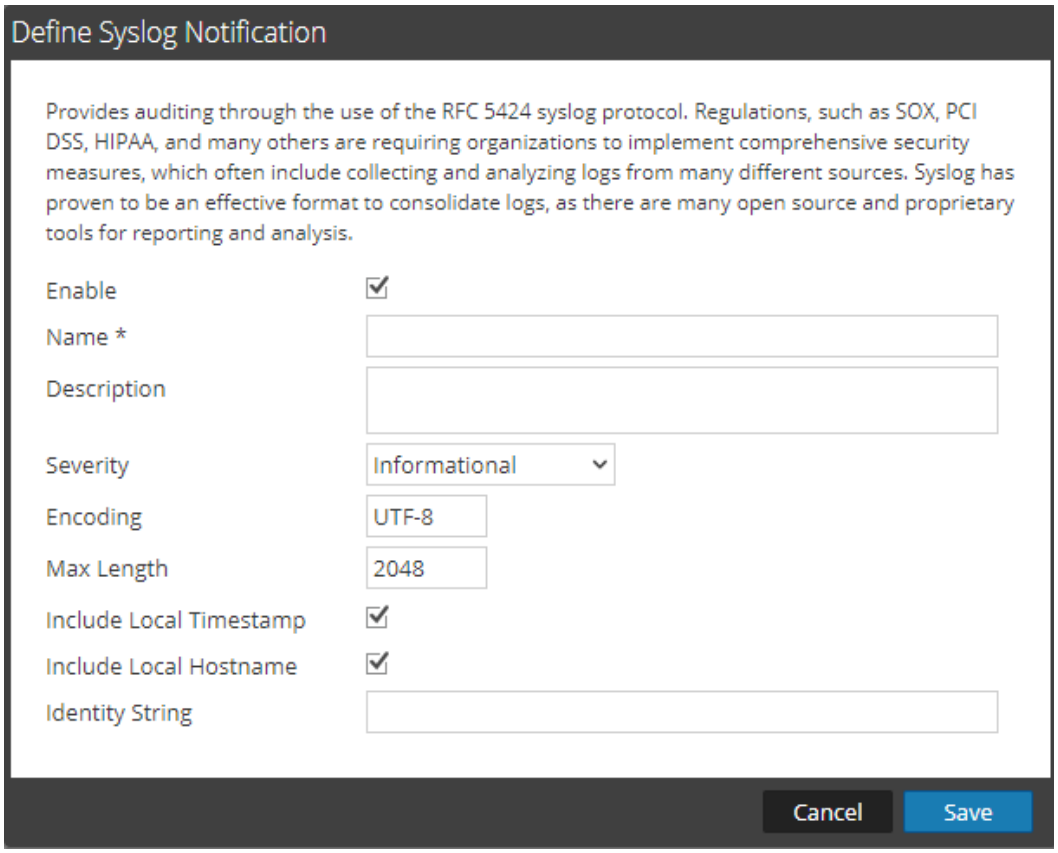
4. In the SNMP Notification dialog, provide the required information and click **Save**.
   For details of the parameters and descriptions, see Define Notification Server Dialogs.

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**.



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** > **Global 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
- New Health & Wellness Alarms.

You can use the available default templates or you can configure your own templates for Email (SMTP), SNMP, Syslog, and Script, depending on the template type. To learn how to modify or configure your own template, see Define Notification Template Dialog.

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 with ESA Correlation Rules User Guide*. You cannot delete templates associated with global audit log configurations.

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

Note: New Health and Wellness supports only Email and Syslog notification outputs.

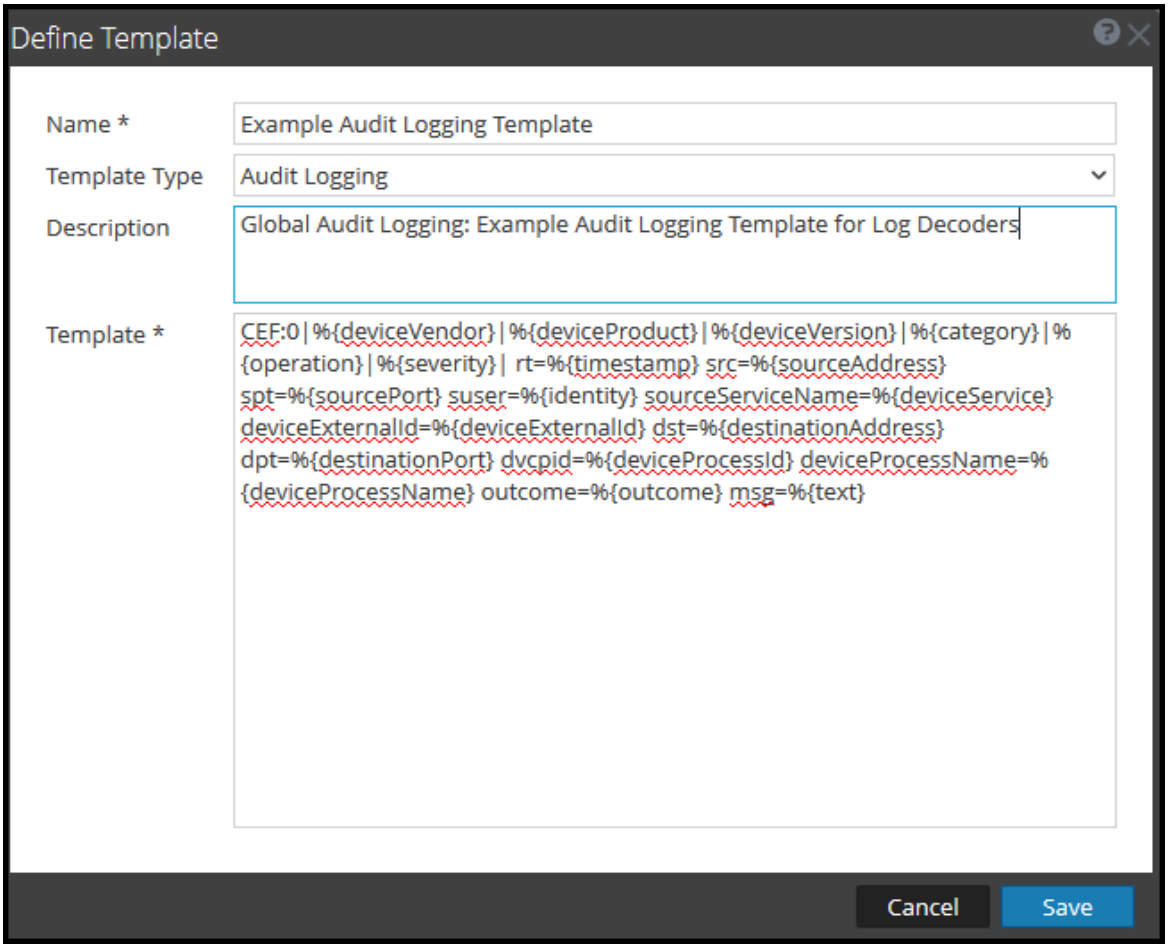
Note: ESA SNMP notifications are not supported for NetWitness 11.3 and later.

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. For New Health and Wellness, select New Health & Wellness Alarms 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, see Define Notification Template Dialog.

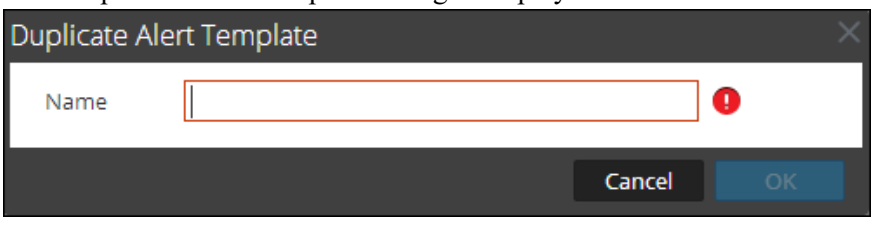
e. Click **Save** to save the template.
The following is an example of a template for Audit Logging.



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.



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')
@RSAAlert(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 has two constituent events, each resembling a NextGen session with multiple meta values. The alert data-object passed to the FreeMarker template evaluator are as follows:

```
(root)
  |
  +- id = "4e67012f-9c53-4f0b-ac44-753e2c982b79"                    // Unique identifier for each alert
  |
  +- severity = 1                                                    // The severity of the alert
  +- time = 2018-12-31T11:02Z                                        // 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 consituent
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 map 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 ...` 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 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 **Select File**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. NetWitness Platform can send notifications to users through 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.

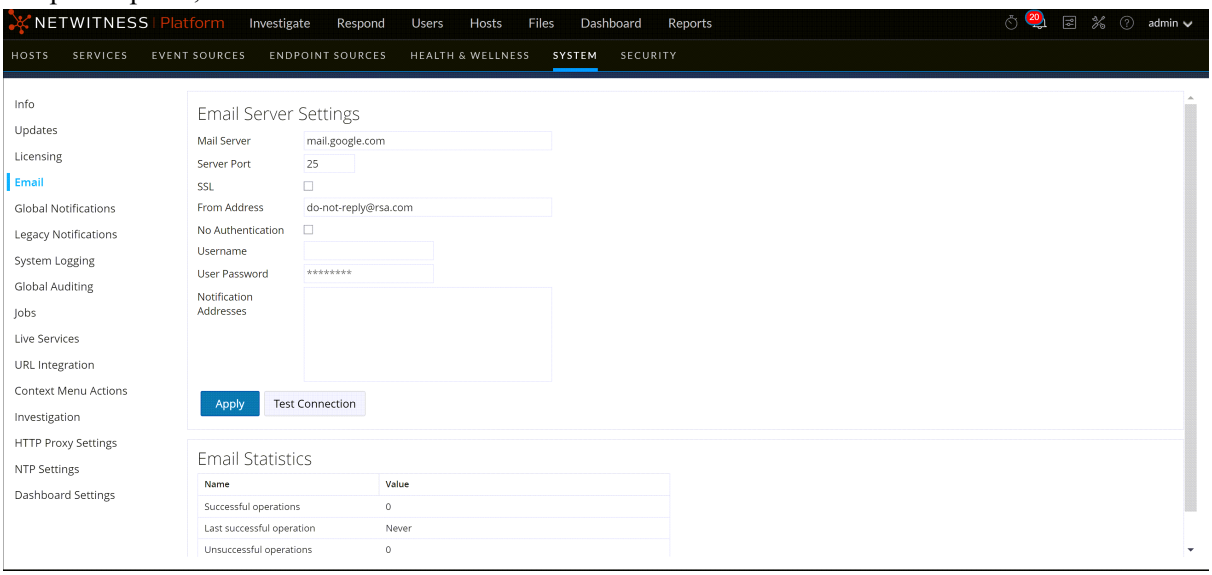
NetWitness requires access to an SMTP mail server in order to send reports to users. Each user account can be configured to receive emailed reports. These reports can be generated manually, through the user interface, or automatically, through the auditing system. The following guidelines apply:

- 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 reports.

To configure NetWitness email notifications:

1. Go to **(Admin) > System**.
   The Administration System view is displayed.

2. In options panel, select **Email**.



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 using SSL, set the box next to **Use SSL**.
5. In the **From address** field, type the name of the email account sending NetWitness 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 modules to receive various notifications by email.

Configure Global Audit Logging

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

NetWitness 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:

- User logouts
- All UI pages accessed
- Committed configuration changes
- Queries performed by the user
- Data export operations

Note: For examples of some of the user actions logged, see Add New Configuration Dialog

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 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 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 ( (Admin) > 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.	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. Configure a Destination to Receive Global Audit Logs. 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.
2. Select or configure an Audit Logging template to use.	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. Configure Templates for Notifications provides additional information. For Log Decoders, 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. 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.
3. (Optional - Only if consuming with a Log Decoder) Deploy the Common Event Format parser to your Log Decoder from Live.	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.

Procedures	Reference / Instructions
4. Define a global audit logging configuration, which defines how the global audit logs are forwarded to external Syslog systems.	Define a Global Audit Logging Configuration 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. Verify Global Audit Logs 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.

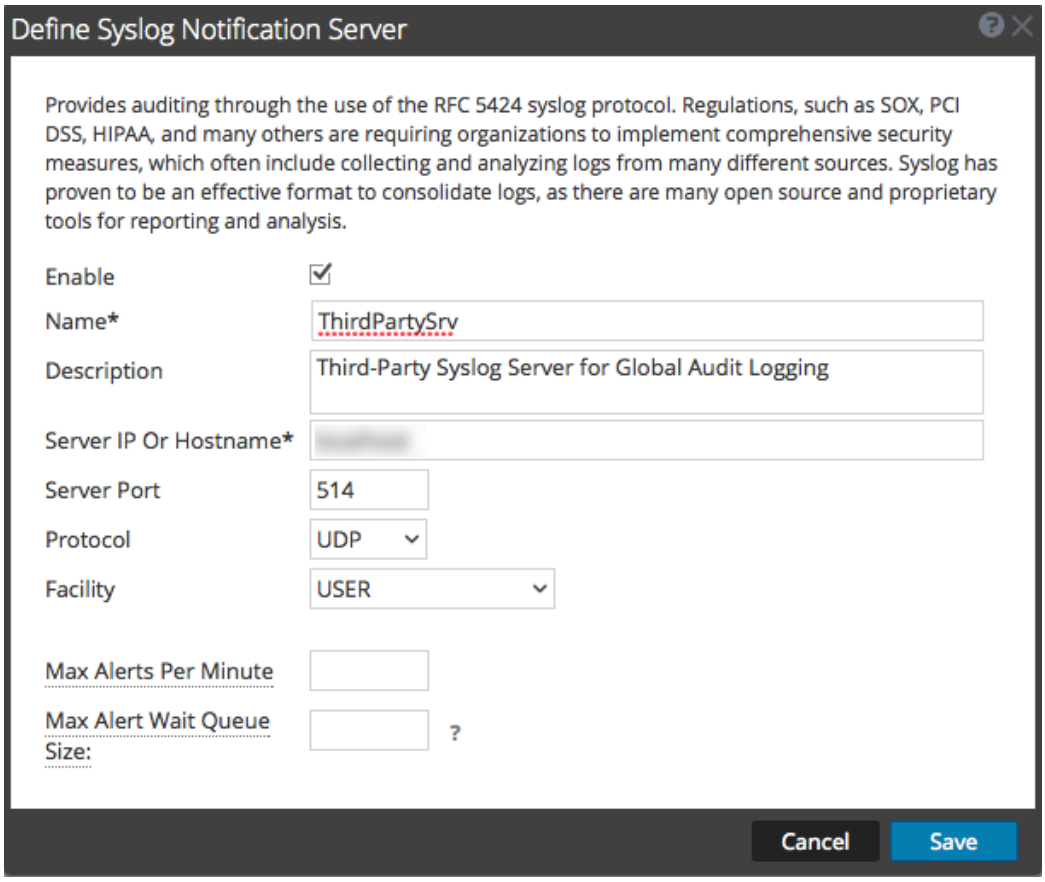
Configure a Syslog Notification Server for a Third-Party Syslog Server

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.



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**.

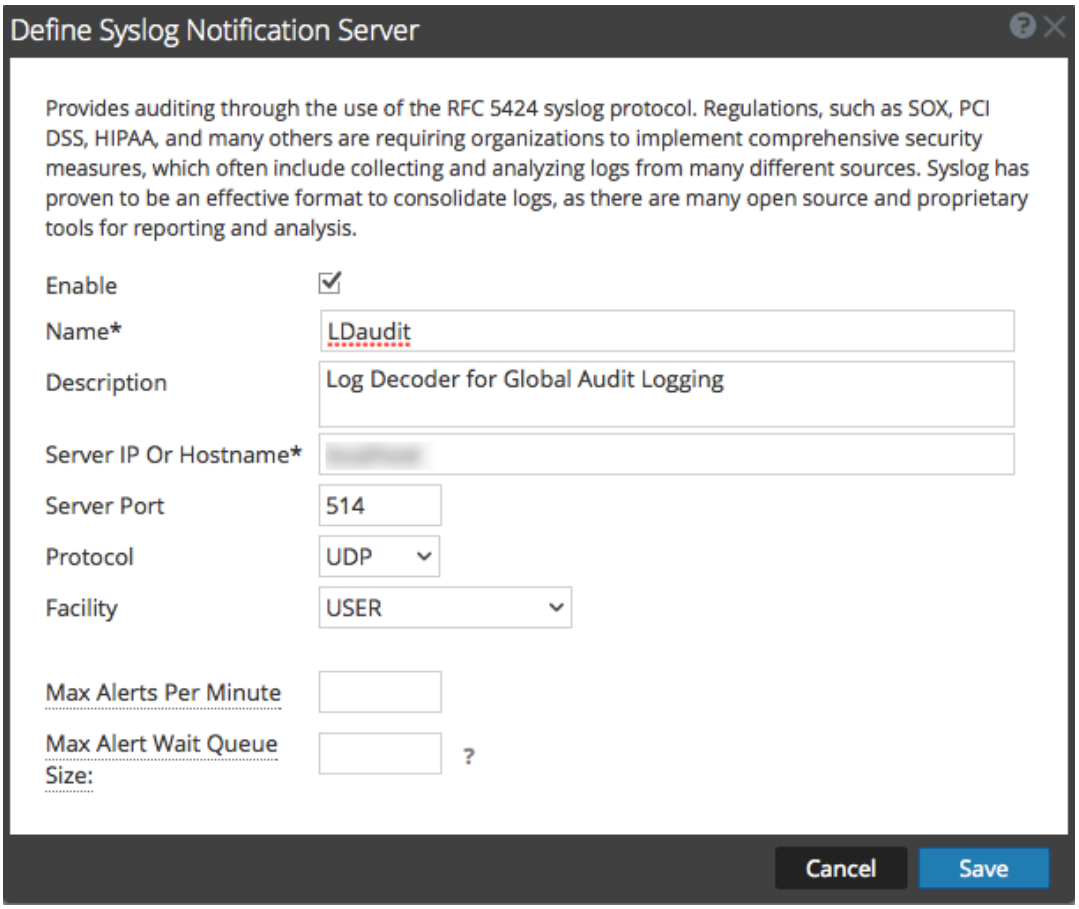
Configure a Syslog Notification Server for a Log Decoder

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.



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.

Field	Description
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 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} dpt=
%{destinationPort} dst=%{destinationAddress} dvcpid=%{deviceProcessId}
tpt=%{transportProtocol} sessionId=%{sessionId} scope=%{scope} suser=
%{identity} sourceServiceName=%{deviceService} deviceExternalId=
%{deviceExternalId} deviceProcessName=%{deviceProcessName} device
Facility=%{deviceFacility} outcome=%{outcome} msg=%{text} remoteAddress
=%{remoteAddress} reasonForFailure=%{reasonForFailure} reason=%{reason}
arguments=%{Arguments} user=%{User} referrerURL=%{referrer} role=%{Role}
id=%{id} account=%{Account} deviceIDs=%{deviceIDs} file=%{file} account
Provider=%{AccountProvider} uri=%{uri} addRole=%{Add.Role} addPermission
=%{Add.Permission} userAgent=%{userAgent} userGroup=%{userGroup}
userRole=%{userRole} key=%{key} value=%{value} paramKey=%{Key}
paramValue=%{Value} alert=%{alert} incident=%{incident} action=%{action}
notification Binding=%{NotificationBinding} name=%{name} enabled=
%{enabled} disabled=%{disabled} params=%{parameters}
```

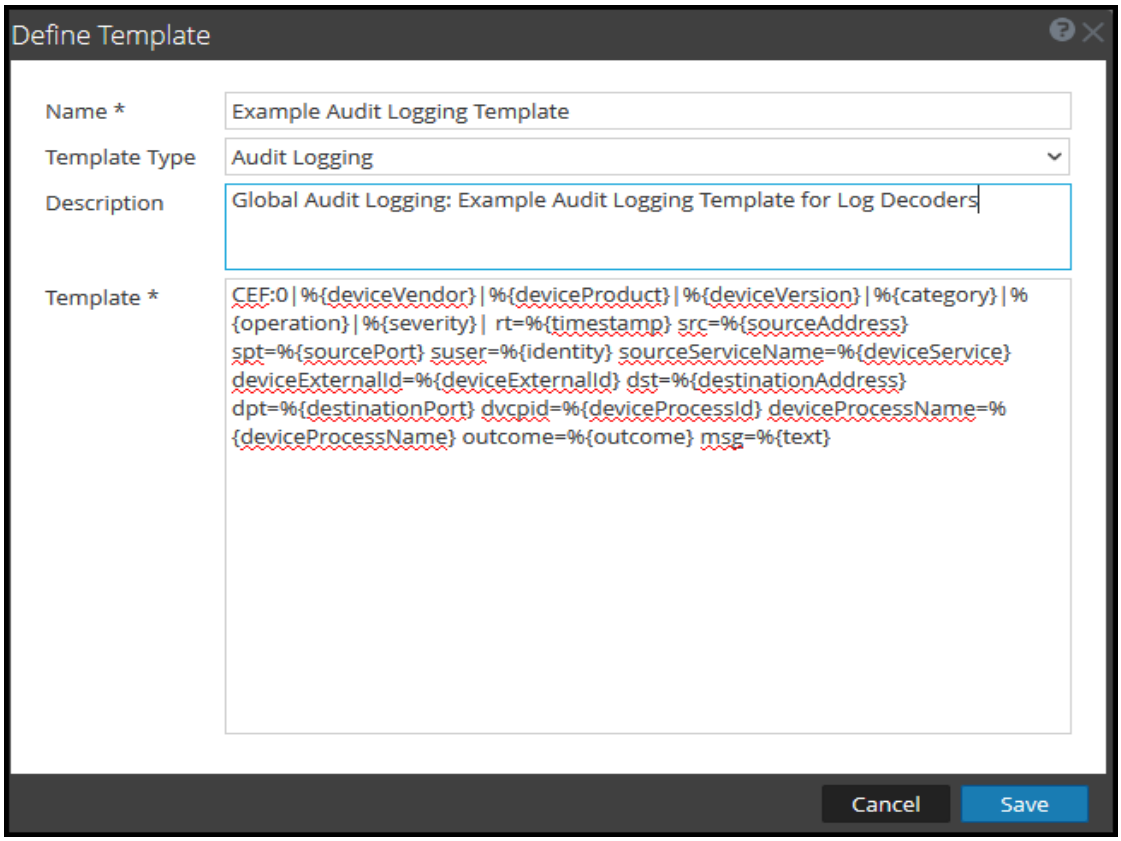
The highlighted CEF syslog header is required to conform to the CEF standard and is a requirement for the CEF parser in the Log Decoder. The other keys are optional and you can configure them. See all the supported meta keys that are supported by the CEF parser in the Log

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.

Note: After you upgrade to 11.x from earlier versions, then '$' is replaced with '%' automatically

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" in the *Live Services Management Guide* provides 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-custom.xml** file on the Log Decoder. If they are not indexed, follow the instructions in 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-custom.xml** on the Concentrator. See the "Edit a Service Index File" topic in the *Host and Services Configuration Guide* for 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.

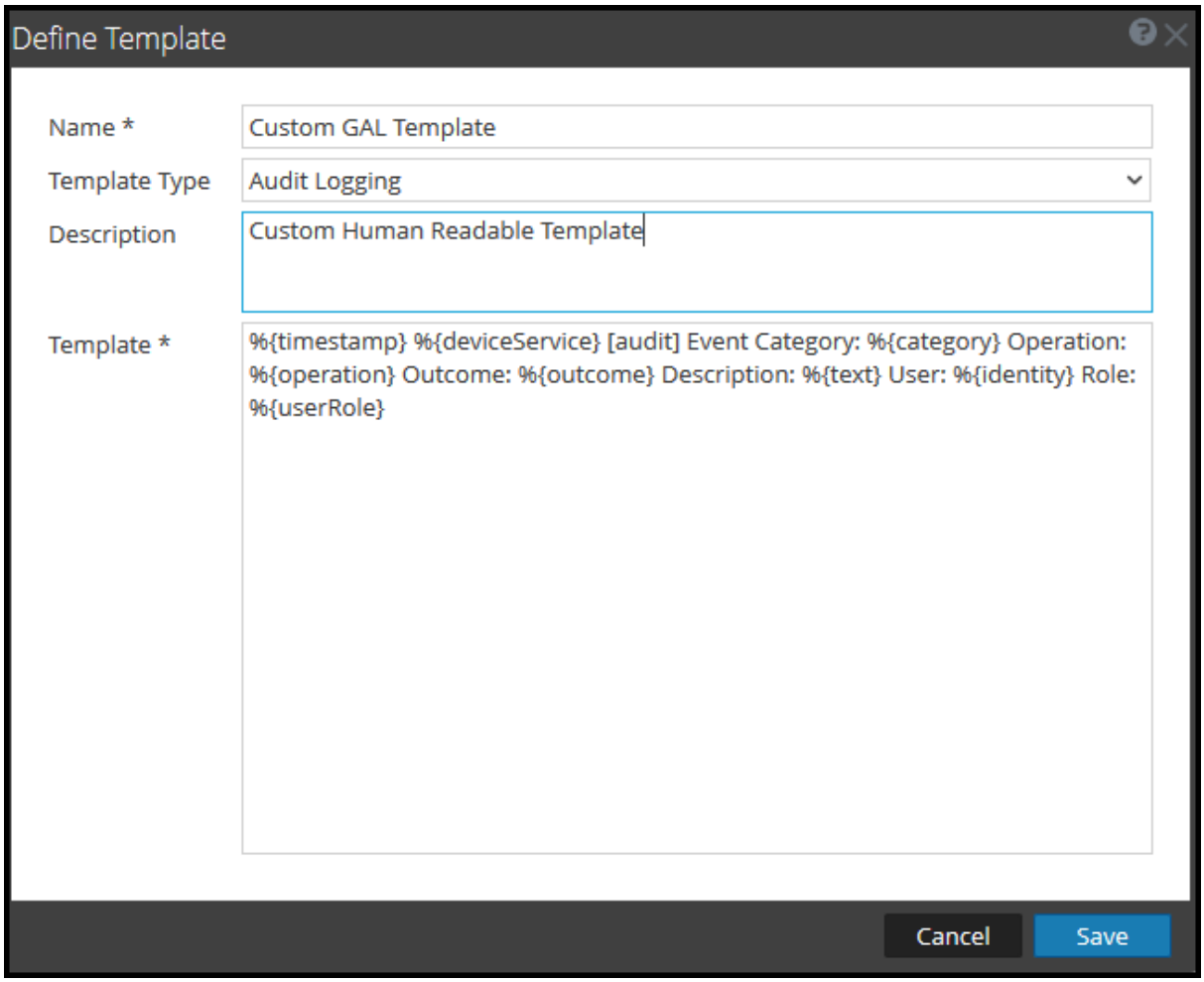
To define a custom global audit logging template in human-readable format:

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} Parameters: %{parameters}
```

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

```
Jun 11 2019 04:53:54 UpdateStackConcentrator Jun 11 2019 04:53:54 CONCENTRATOR
[audit] Event Category: DATA_ACCESS Operation: sdk.info Outcome: pending
Description: has requested the SDK summary info User: admin Role: null
params=flags\=1
```

```
Jun 11 2019 04:53:55 updatestackadminserver Jun 11 2019 04:53:55 source-server
[audit] Event Category: API Operation: /rsa/process/ready Outcome: success
Description: null User: Netwitness Web(nw-web) Role: null params=
{"Arguments":"[]"}
```

```
Jun 11 2019 05:15:46 UpdateStackeplh Jun 11 2019 05:15:46 LOG_DECODER [audit]
Event Category: MANAGEMENT Operation: upload Outcome: pending Description: has
started uploading file User: escalateduser Role: null params=file\=esmFeed.zip
```

Next Step

Define a Global Audit Logging Configuration provides instructions for defining a global audit logging configuration for NetWitness.

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

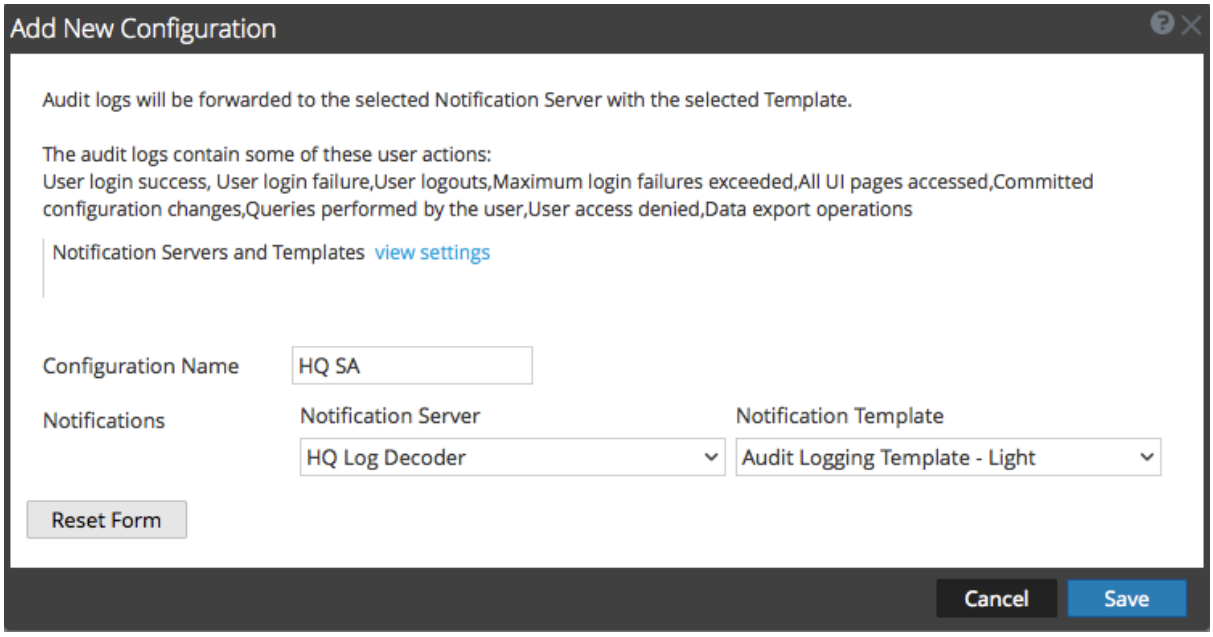
You configure the notification server and template on the Global Notifications panel. You can access the Global Notifications panel by going to (Admin) > System and select Global Notifications. You can only define a Syslog type of Notification Server for global audit logging. For Log Decoders, use a 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 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 components, see Global Audit Logging Operation Reference.

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 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.

In version 11.5 and later, audit logging provides information about the aggregation account and the actual user who submitted the query. For example, the information is displayed as follows in the audit log:

```
User aggAccount (session 478, [::1]:1133, on behalf of <username of submitter>) has requested the SDK transforms.
```

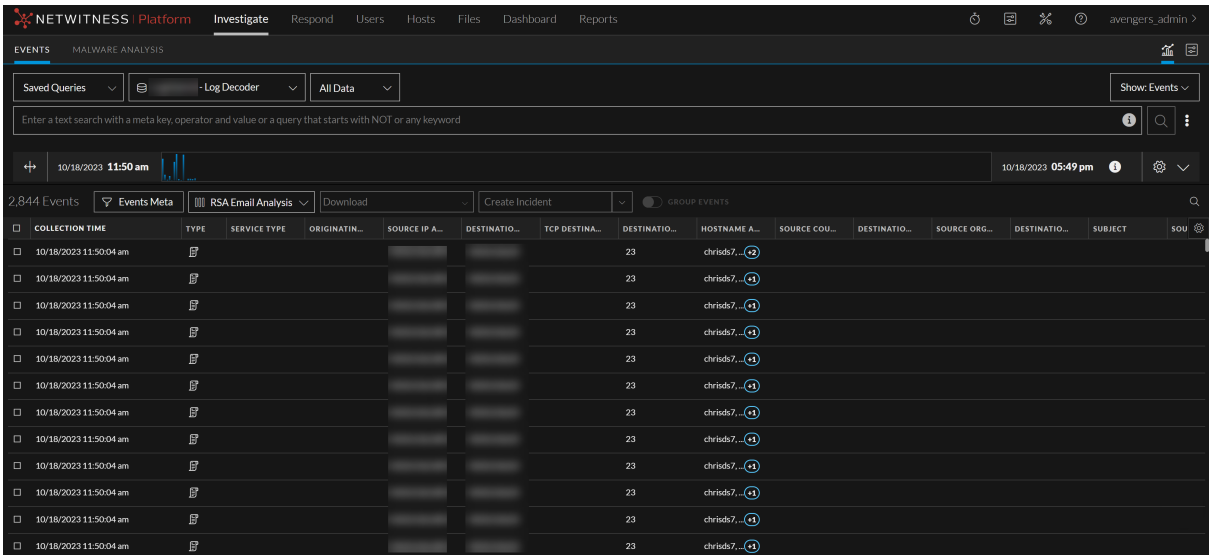
This information is available through multiple levels of Brokers and Concentrators.

Note: If you are running a mixed-version environment, any version earlier than 11.5 will not provide the real user information.

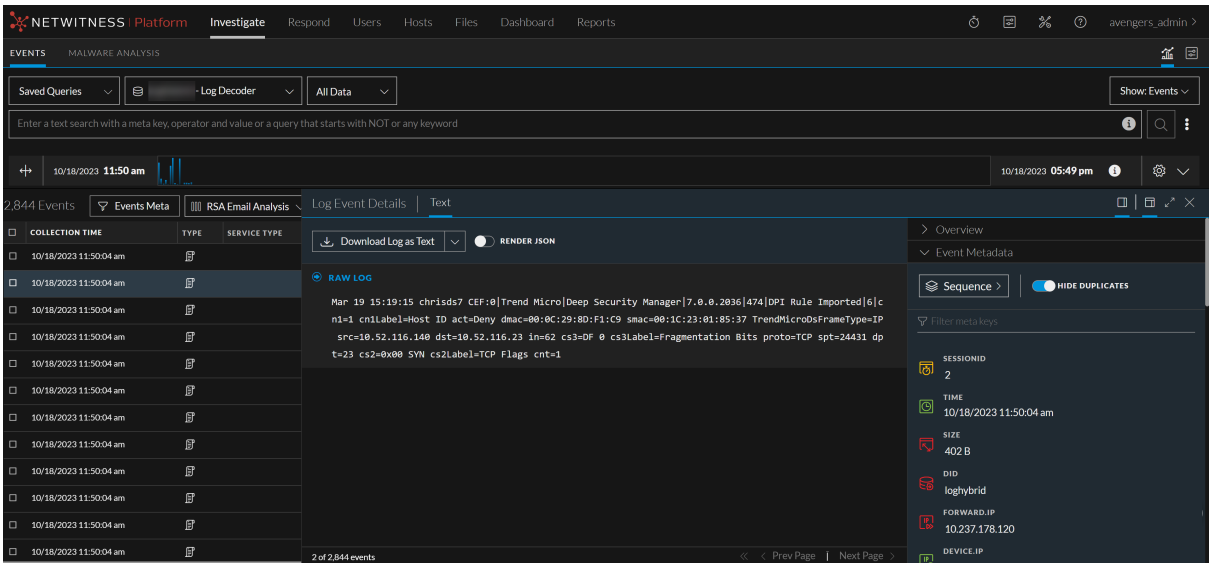
Before starting this task, complete the steps detailed in Configure Global Audit Logging.

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

1. Go to **Investigate** > **Events**, select the Log Decoder service and click the submit query icon () to the right of the query bar.



2. 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.
3. Double-click a log to open the reconstruction and click  to open the Event Meta panel.
4. 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}|%{operation}|%{severity}|
```

```
t=%{timestamp} src=%{sourceAddress} spt=%{sourcePort} tpt=%{transport
Protocol} scope=%{scope} suser=%{identity} sourceServiceName=%{device Service}
deviceExternalId=%{deviceExternalId} deviceProcessName=%{device ProcessName}
outcome=%{outcome} msg=%{text} remoteAddress=%{remoteAddress}
reasonForFailure=%{reasonForFailure} reason=%{reason} arguments= %{Arguments}
user=%{User} referrerURL=%{referrer} role=%{Role} id=%{id} account=%{Account}
deviceIDs=%{deviceIDs} file=%{file} accountProvider= %{AccountProvider} uri=%
{uri} addRole=%{Add.Role} addPermission= %{Add.Permission} userAgent=%
{userAgent} userGroup=%{userGroup} userRole= %{userRole} key=%{Key} value=%
{Value} alert=%{alert} incident=%{incident} action=%{action}
notificationBinding=%{NotificationBinding} name=%{name} enabled=%{enabled}
disabled=%{disabled} params=%{parameters}
```

Example logs:

```
Jun 07 2019 09:06:05 UpdateStackConcentrator CEF:0|RSA|NetWitness Audit|
11.3.1.0|AUTHENTICATION|logoff|6|rt=Jun 07 2019 09:06:05 src=101.101.101.
101 spt=55060 scope=scope suser=admin sourceServiceName=CONCENTRATOR
deviceExternalId=3ebf91d9-e879-4727-a473-72d309e1741d deviceProcessName=
NwConcentrator outcome=success \r\n
```

```
Jun 07 2019 09:06:11 UpdateStackConcentrator CEF:0|RSA|NetWitness Audit|
11.3.1.0|AUTHENTICATION|login|6|rt=Jun 07 2019 09:06:11 src=101.101.101.101
spt=55060 scope=scope suser=admin sourceServiceName=CONCENTRATOR device
ExternalId=3ebf91d9-e879-4727-a473-72d309e1741d deviceProcessName=
NwConcentrator outcome=success userGroup=Administrators userRole=admin.owner,
aggregate,concentrator.manage,connections.manage,database.manage,everyone,
index.manage,logs.manage,rules.manage,sdk.content,sdk.manage,sdk.meta,
sdk.packets,services.manage,storedproc.execute,storedproc.manage,sys.manage,
users.manage \r\n
```

Configure Centralized Audit Logging

NetWitness Platform collects audit logs from all the NetWitness services and aggregates it into a single file in a centralized location on the NetWitness Admin Server. This aggregated log file provides the advantage for faster access and easy analysis of the audit logs.

The aggregated logs from all services are sent to the following centralized location:

- `/var/netwitness/logstash/logs/rsa-netwitness-audit.log` (JSON format)
- Syslog running on the local host (human-readable format)

Centralized audit logging is enabled by default. To forward the aggregated logs to the external syslog system (a third-party Syslog server or Log Decoder), you must configure the Global Audit logging in  **(Admin) > System > Global Auditing**. The aggregated logs are sent in the format specified in the selected Audit Logging template. A Syslog Notification Server configuration defines the destination to send the audit logs. To forward the audit logs to a Log Decoder, configure a Syslog type of Notification Server for the Log Decoder.

- For instructions on how to define a template, see Define a Template for Global Audit Logging
- For instructions on how to configure a syslog notification server, see Configure a Destination to Receive Global Audit Logs
- For instructions on how to configure global Audit logging, see Define a Global Audit Logging Configuration

Filtering the Aggregated Logs

Before the logs are aggregated, standard filters are applied to the logs to reduce redundancy and filter out logs that are not useful. The filters contain entries that control the content written to the aggregated log file. The following default filters are available in `/etc/logstash/` location.

- `json-filter-action.yaml`
- `json-filter-category.yaml`

`json-filter-action.yaml` - This filter blacklists the log messages based on the `operation` meta key and stops the log message being written to aggregated log file. For example, if `"/rsa/process/ready":"true"` is entered in `json-filter-action.yaml`, any raw log that contains `"/rsa/process/ready"` in the `operation` meta key is blacklisted and not written to aggregated log file.

Note: If you do not want to apply filters, then delete all the default entries and replace with `{}` character. Note that this increases the log size and the logs may be redundant.

`json-filter-category.yaml` - This filter whitelists the log messages based on the `category` meta key and writes the log message to the aggregated log file. For example, if `'\b(?i)SECURITY\b':"true"` is entered in `json-filter-category.yaml`, any raw log that contains `'SECURITY'` in the `category` meta key is whitelisted and written to the aggregated log file.

Log Retention Policy

The aggregated log file is retained as per the following default settings:

- If the file size reaches 250 MB, the file is compressed as a single zip file.
- If the number of zip files exceed 90, the oldest zip file in the directory is automatically deleted.

You can modify the log retention policy in the file `logstash` available in `/etc/logrotate.d/` location.

Note: The size of the aggregated log file depends on the filters applied, so make sure to set up filters correctly for optimal directory space.

Disable Centralized Audit Logging

If you do not want the logs to be aggregated, in the `json-filter-category.yaml` filter, delete all the default entries and replace with the `{}` character.

Configure Investigation Settings

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

Map Context Hub Meta Types

The Context Hub is preconfigured with meta fields mapped to entities. NetWitness Respond and Investigate use these default mappings for context lookup. For information about adding meta keys, see "Configure Context Hub Data Source Settings" in the *Context Hub Configuration Guide*.

Caution: For the Context Lookup to work correctly in the Respond and Investigate views, when mapping meta keys in the  (Admin) > System > Investigation > Context Lookup tab, it is best practice to add only meta keys to the Meta Key Mappings. Do not add fields in the MongoDB to the Meta Key Mappings. Here is a sample meta key and Mongo DB field; `ip.address` is a meta key and `ip_address` is a field in the MongoDB.

In the **Context Lookup** tab, you can manage mapping of Context Hub meta types with meta keys in Investigate. You can add or remove meta keys in the list of meta types supported in Investigate by Context Hub. Procedures associated with this tab are provided in "Manage Context Hub Lists and List Values in the Navigate and Events Views" in the *NetWitness Investigate User Guide*.

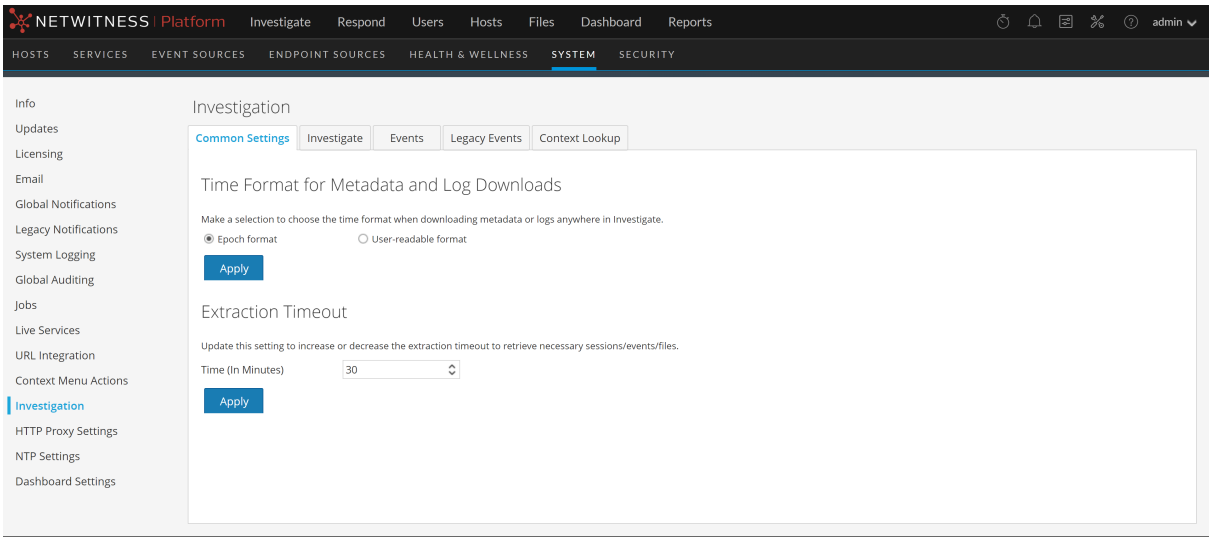
Configure Common Settings

In version 11.5 and later, the Common Settings tab allows you to configure settings that apply to the Navigate view, the Events view, and the Legacy Events view. Initially, the only setting that you can set for all views is the time format used when downloading metadata and logs, and other settings may be added in future versions.

By default, the time format for downloads is Epoch format, which shows the time as a numerical value representing the number of seconds from the Unix epoch, January 1, 1970. The resulting number requires a conversion to be understood. You can change the setting to get a more understandable format that combines the user preference time zone, date format, and time format into an easily understood representation, which follows the industry standard ISO 8601 representation when possible.

This setting applies to all 11.7 Investigate views.

1. Go to **(Admin) > System**, and in the options panel, select **Investigation**.
   The Investigation Configuration panel is displayed.



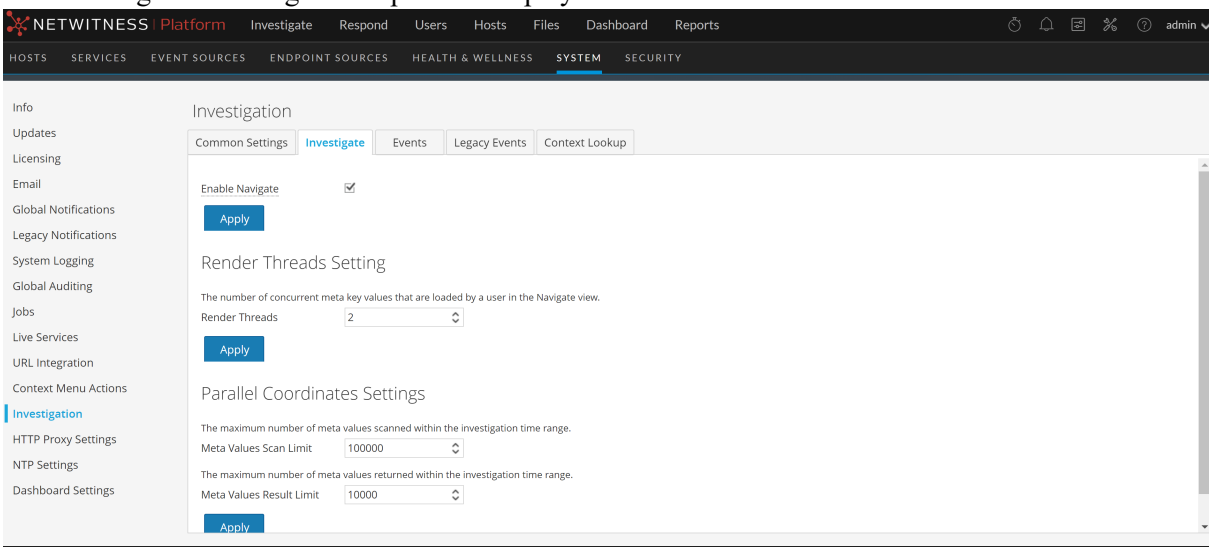
2. In the **Common Settings** tab, do the following:
   a. Select the time format to be used in metadata and log downloads in Investigate.
   b. Edit the time in minutes to set the extraction timeout when the logs are downloaded before the session expires.
      By default, it is set to 30 minutes and can be set to a maximum of 60 minutes.
3. Click **Apply**.
   The setting goes into effect immediately.

Configure Navigate and Legacy Events View Settings

The name of the Version 11.3 and earlier Events tab was changed to Legacy Events tab in Version 11.4.

1. Go to **(Admin) > System.**
2. In the options panel, select **Investigation.**

The Investigation Configuration panel is displayed.



3. In the **Investigate** 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**.
4. In the **Investigate** 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**.
5. In the **Legacy Events** tab, in the **Enable Legacy Events** section, select the check box to view the legacy sub menus and legacy events in classic view. Click **Apply**.
6. In the **Legacy 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 Legacy Events view. The actual number of events scanned and displayed may be slightly greater than the limit set here. Click **Apply**.
7. In the **Legacy 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 500 maximum packets and 2097152 bytes. If analysts are seeing slow performance when reconstructing sessions in Investigate, the reconstruction 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 **Legacy 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**.

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 Investigate is browsing a Broker and a downstream Concentrator or Decoder has a data reset, the metadata and session data for the investigating service (Broker) does not match the content if the downstream service has reset and repopulated. The reconstruction in Investigate 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 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 because NetWitness can reuse service IDs. In this case, clearing the cache on the Broker causes NetWitness to request data from the services.

To clear reconstruction cache, do one of the following:

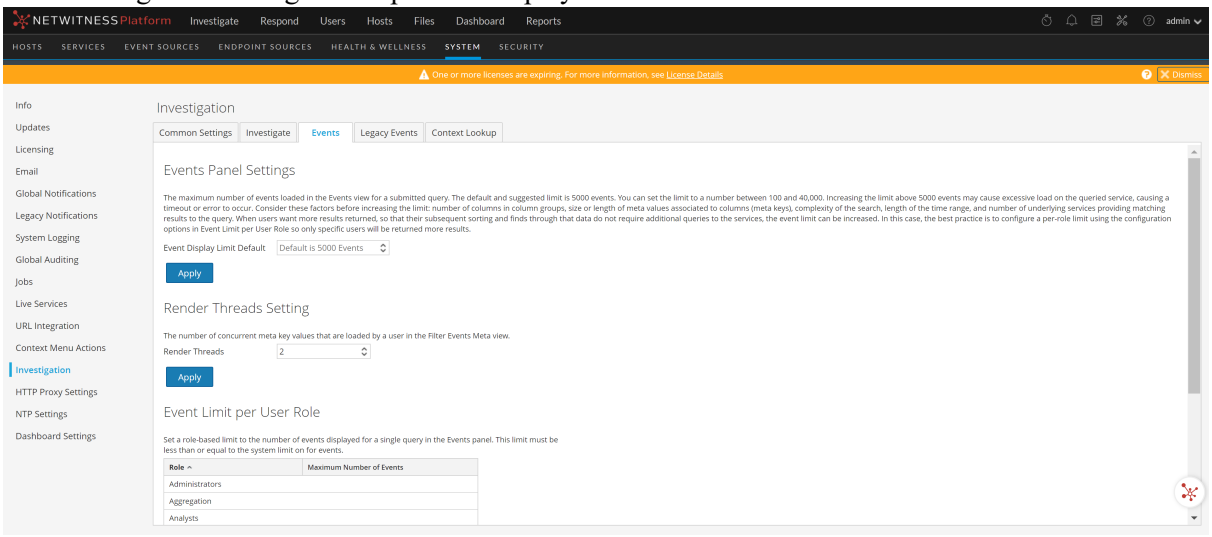
1. To clear cache for one or more services, select the services and click **Clear Cache for the Selected Services**.
2. To clear the cache for all listed services, click **Clear Cache for All Services.**
   The reconstruction cache for the selected services is cleared. NetWitness sends a request for data to the services.

Configure Events View Settings

These settings apply to the 11.3 and earlier Event Analysis view and the 11.4 and later Events view.

1. Go to **(Admin) > System**, and in the options panel, click **Investigation**.

   The Investigation Configuration panel is displayed.



2. In the **Events** tab, in the **Event Display Limit Default** field under **Events Panel Settings**, select the maximum number of events loaded in the Events panel when a query is submitted.
   The default and suggested value is 10,000 events, and you can select a value between 100 and 40,000 events. Increasing the limit above 10,000 events may cause excessive load on the queried service, causing a timeout or error to occur. Consider these factors before increasing the limit: number of columns in column groups, size or length of meta values associated to columns (meta keys), complexity of the search, length of the time range, and number of underlying services providing matching results to the query.
   When users want more results returned, so that their subsequent sorting and finds through that data do not require additional queries to the services, the event limit can be increased. In this case, the best practice is to configure a per-role limit using the configuration options in Event Limit per User Role so only specific users are returned more results. For example, set the global Event Limit Default to 5,000, and then create different Analyst roles that can be set to higher limits, up to the maximum 40,000 events.
3. If a query returns more events than the configured Event Limit Default, the Events panel title shows the analyst that more results are available but are not listed due to the limit. Increasing the limit may place additional load on the queried service; the ideal limit is determined by your environment.
4. Click **Apply**.

   The change becomes effective immediately, and applies to any new queries submitted by analysts.
5. Under **Render Threads Settings** in the **Render Threads** field, select the maximum number of concurrent meta key values that are loaded by a single user in the Events Meta view. The Render Threads value should be between **1-8**. The default value is **2**.

   Note: By increasing the number of render threads, the meta values within the Events Meta panel are loaded simultaneously.
6. Click **Apply**.

The change becomes effective immediately, and applies to any new queries submitted by analysts.

7. Under **Event Limit Per User Role**, select the maximum number of events loaded for a single query for individual user roles. This limit must be less than or equal to the system events limit of 40,000 events; it can be larger than the default or configured limit set under Event Limit Default.
8. Click **Apply**.

   The change becomes effective immediately, and applies to any new queries submitted by users assigned to the user role.

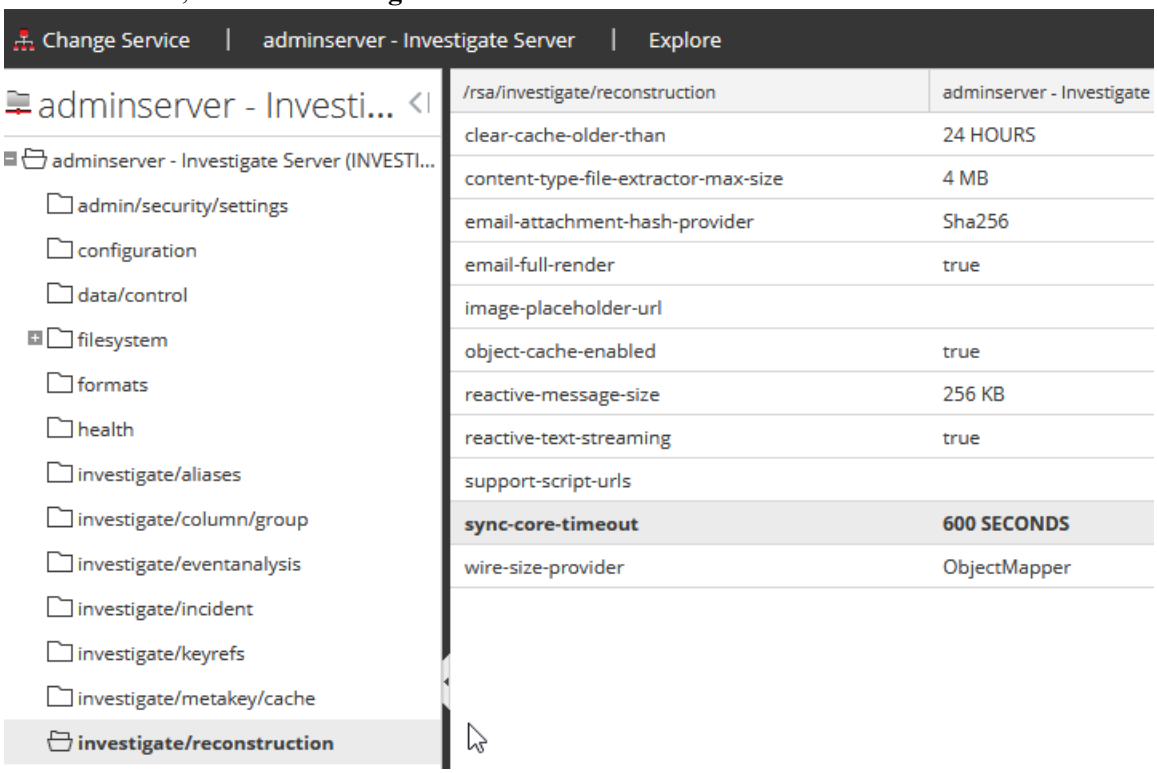
Configure the Sync Core Timeout to Remedy Deadlocks in Events View Reconstructions

The `sync-core-timeout` is a setting in the `/investigate/reconstruction` node that determines the maximum time to wait for operations for caching core content to complete to prevent deadlocks. The default value is 600 seconds (10 minutes) and needs no adjustment under most circumstances. If analysts are seeing a spinner for a very long time (>10 minutes) when loading a reconstruction in the Events view, for example from events on a 10G Decoder, increasing the length of this timeout may improve the ability to reconstruct events.

Caution: Changing the timeout setting to more than 600 seconds may lead to stability issues.

To adjust the sync-core-timeout:

1. Go to  **(Admin) > Services > Investigate-server** and **View > Explorer**.
2. In the node list, click the **investigate-reconstruction** node.



3. In the **sync-core-timeout** field, type a new value for the number of seconds before timeout and press **RETURN**.
   The setting is applied and goes into effect immediately.

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 (Version 11.4.0 and earlier).
- Sharing Live Content Usage
- RSA Live Connect (Version 11.5.0 and earlier).

Prerequisites

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

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

About Live Feedback Participation

Once you sign up for a Live account, Live Feedback automatically collects relevant information for further improvement and anonymously sends it to NetWitness. The shared data is protected in accordance with the applicable license agreement. For information on Live Feedback, see Live Feedback Overview. For information, see Configure Live Services Settings

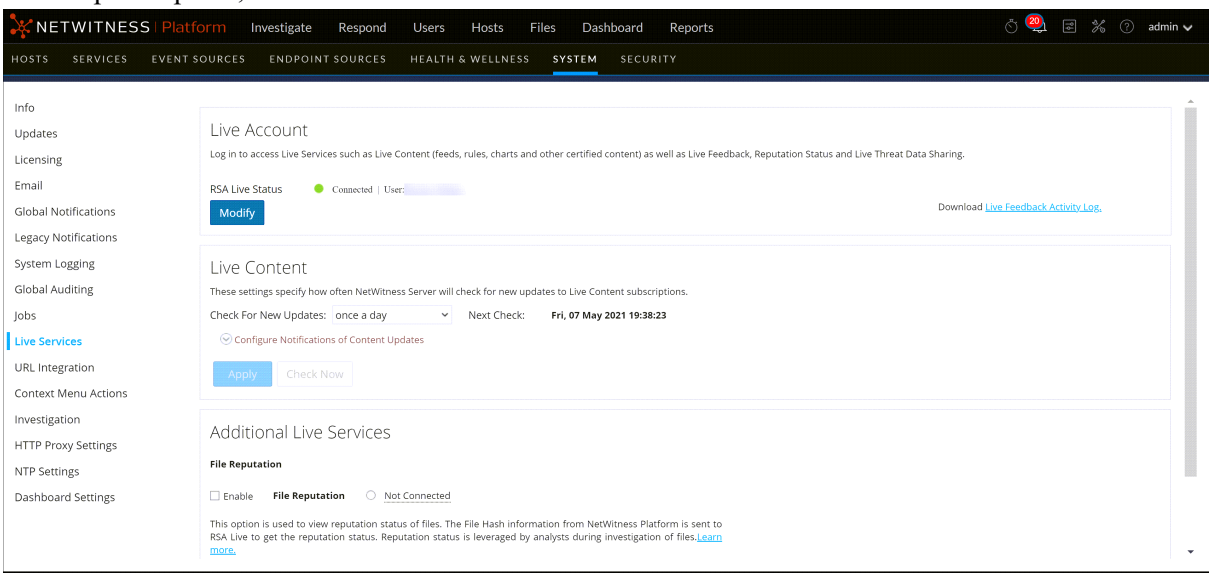
If needed, you can manually download historical usage data and share it with NetWitness. For information on how to download historical usage data and share it with NetWitness, see Upload Data to NetWitness for Live Feedback.

This topic contains the following procedures:

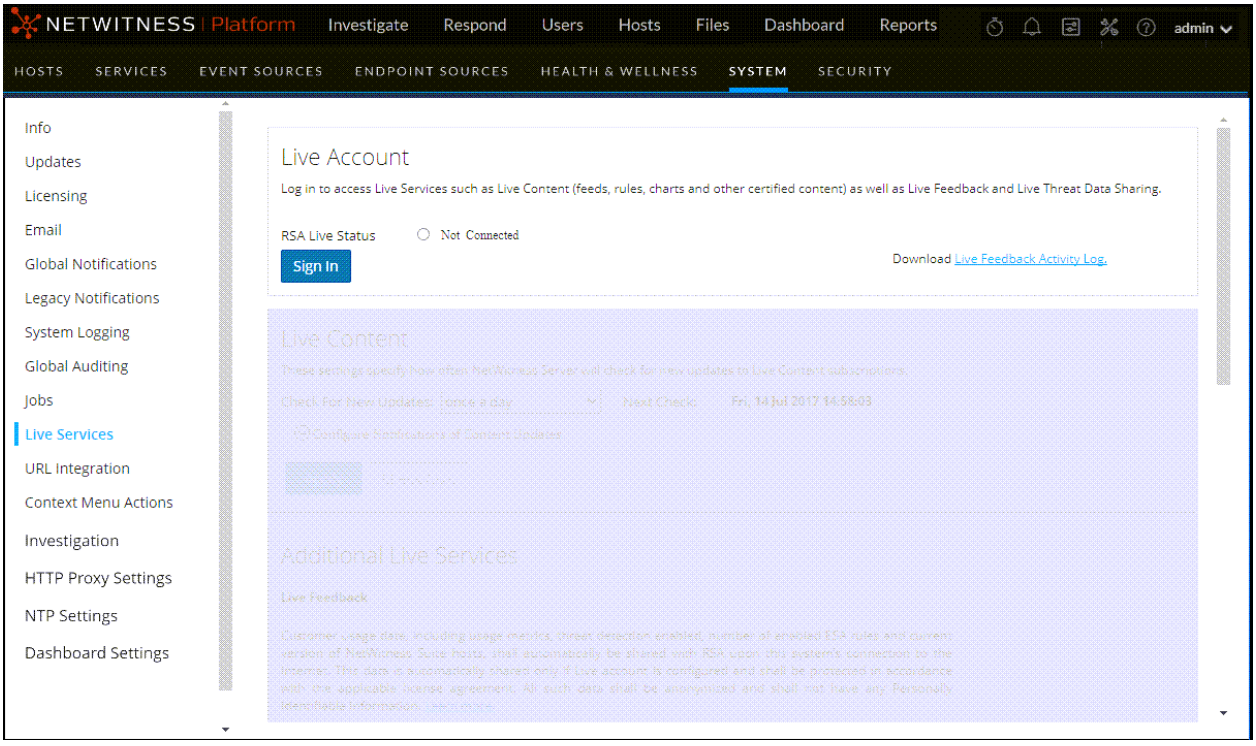
- Access the Live Services Configuration Panel
- Configure Live Account
- Configure the Live Content Synchronization Interval and Notification
- Force Immediate Synchronization

Access the Live Services Configuration Panel

1. Go to  **(Admin) > System**.
2. In the options panel, select **Live Services**.



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



Configure Live Account

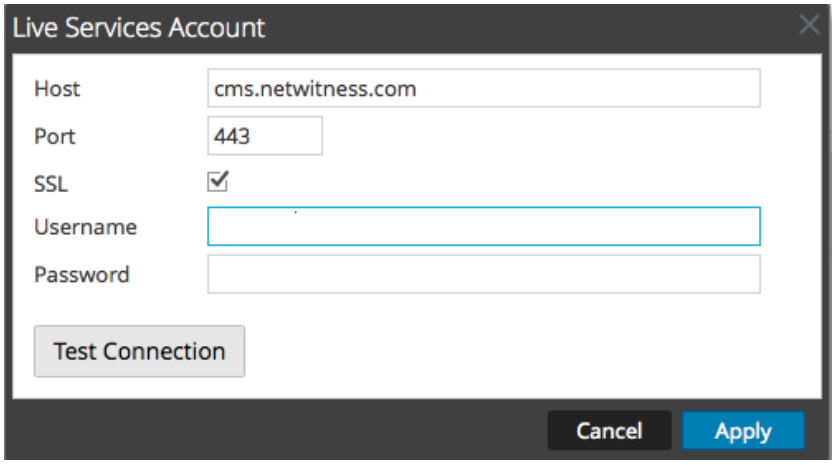
In the **Live Account** section, you must set up the user's Live account. The information needed to set up the user's Live account consists of the Username, Password, and Live URL for the Content Management System. This information is provided by Customer Care.

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.

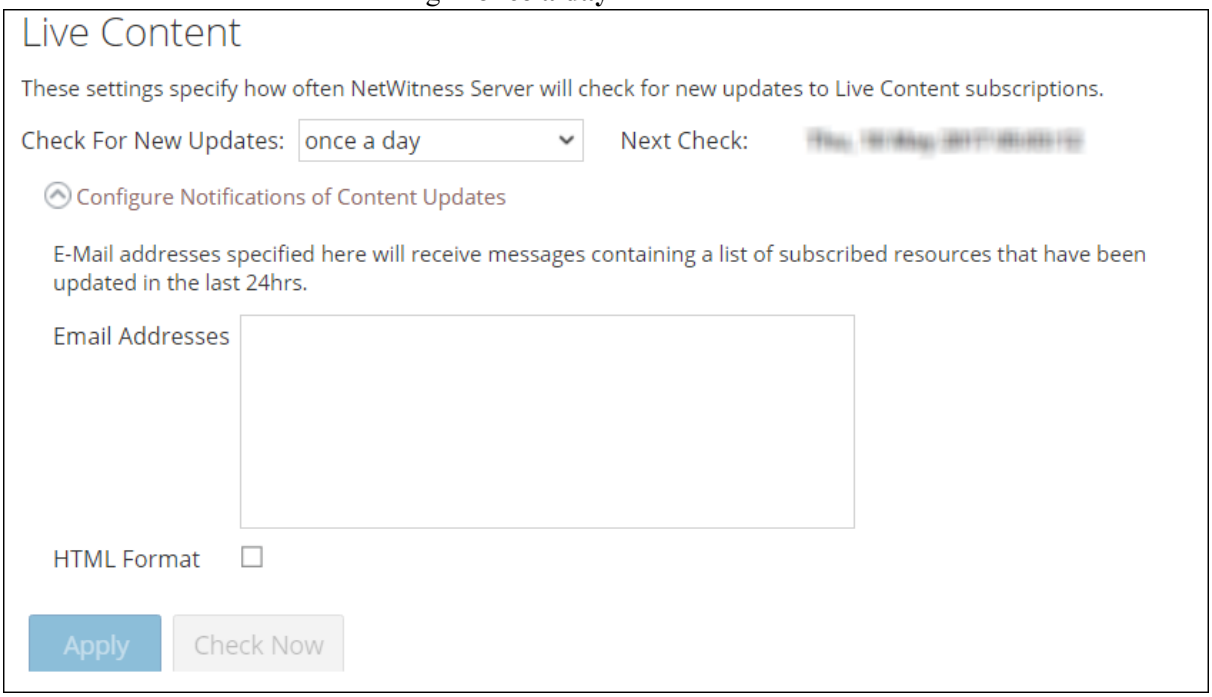


3. (Optional) If you are using a different CMS, type the host URL for the Content Management System. The default points to the CMS at **cms.netwitness.com**.
4. (Optional) If you are using a different CMS, type the communications port for Live to send requests to the Content Management System. The default 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 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**.



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. 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 checks for updates in subscribed resources.

File Reputation

File Reputation provides analysts the opportunity to view reputation status of files.

By default, **File Reputation** is enabled in **Additional Live Services** section.

Live Feedback Overview

This topic provides an introduction to Live Feedback. Live Feedback collects relevant information such as the Licensing usage data for Network 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. For more information about the licensing usage data for Packer Decoder, Log Decoder and Malware Analysis, see the **License Details** tab topic in the *Licensing Guide*. The information is collected to improve future releases of NetWitness. 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 NetWitness. Live Content usage metrics for resource types from  **(Configure) > Live Content > Search Criteria** such as total count of NetWitness Application Rule, NetWitness Correlation Rule etc. can be shared with NetWitness. 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

Once you sign up for a Live account, Live Feedback automatically collects relevant information for further improvement and anonymously sends it to NetWitness. The shared data is protected in accordance with the applicable license agreement. For information on Live Feedback, see Live Feedback Overview. For information, see Configure Live Services Settings

If needed, you can manually download historical usage data and share it with NetWitness. For information on how to download historical usage data and share it with NetWitness, see Upload Data to NetWitness 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 NetWitness 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 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 deployment. For example, 11.1.0.0.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	• **Name** - This is the name of the property for that component. For example, malware analysis, ESA, log decoder, etc. • **Value** - This is the unique value to identify the component.

Metrics

Metrics of the components (hosts) such as Log Decoder, Decoder and Malware Analysis. The license usage data for each host is shared. For Live Content usage metrics, resource types from  **(Configure) > Live Content > Search Criteria** such as total count of NetWitness Application Rule, NetWitness Correlation Rule and so on are shared.

Component	Description
Usage	• **Value** - This is the value generated for the specific component ID for each component. • **Name** - This is the name of the statistics for which the metrics is collected. For example, Capture Total Bytes.
StartTimeUTC	This is the time from when the metrics is collected. (in EPOCH format).
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.

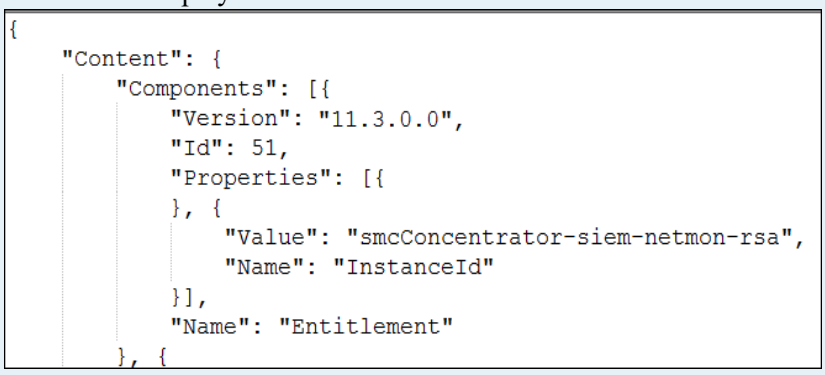
Other Product Details

- **End Time** - This is the time when the metrics collection is complete (in EPOCH format).
- **Product Name** - This is the name of the product. In this example, the Product Type is **NetWitness**.
- **Version** - This is the version of the JSON file which tracks the changes made to the file format.

- **Start Time** - This is the time from when the metrics is collected. (in EPOCH format).
- **Product Type** - This is the name of the product. In this example, the Product Type is **NetWitness**.
- **Product Version** - This is the version of the product from which the metrics is collected. In this example, the Product Version is **11.3.0.0-SNAPSHOT**.
- **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	The details of all the services in NetWitness 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.  **Version**: Displays the version of NetWitness service. For example, 11.3.0.0. **ID**: Displays an unique id which is generated for the NetWitness 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:  **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. For example, For malware analysis the value displayed as "55f7a0b30e502231c42d063f" **Name: "InstanceId"**: Displays the name of the property as shown in the above figure.

Metrics	Description
	Name": "malwareanalysis": Displays the name of component which is a service name such as LogDecoder, Decoder, or MalwareAnalysis.

Metrics	Displays the list of the metrics with the usage data for components namely MacHosts, LinuHosts and WinHosts.
	In this example, the metrics is displayed for ComponentId 1 in bytes.
	 
	}],
	"Metrics": [{
	"Usage": [{
	"Value": "0.0",
	"Name": "MacHosts"
	}, {
	"Value": "0.0",
	"Name": "LinuxHosts"
	}, {
	"Value": "0.0",
	"Name": "WinHosts"
	}, {
	"Value": "0.0",
	"Name": "TotalHosts"
	}],
	"StartTimeUTC": 1539043200000,
	"EndTimeUTC": 1539129599000,
	"ComponentId": 1
	}, {

	StartTimeUTC: Displays the time when the metrics is collected, in the EPOCH format.
	Usage: Displays the usage value and usage type statistics of the component.
	Value: Displays the value of the statistics. For example, "Value": "1582940012678" as shown in the above figure.
	Name: Displays the name of the statistics. For example, Capture Total Bytes or Total File bytes.
	EndTimeUTC: Displays the time when the metrics collection is complete, in the EPOCH format.
	ComponentId: Displays the component id for which the metric values are collected. This is the same as the "ID" in the Components section.
Content	Displays the content that contains all the Components, Metrics, Product Type and Product Instance data except Checksum.
ProductType	Displays the product type that generates the file. For example, `"ProductType": "NetWitness Platform"`
ProductInstance	Displays the License server Id and is unique per NetWitness. For example, `"ProductInstance": "00-0C-29-6C-66-E3"`

Metrics	Description
Checksum	Displays the Checksum for the "Content" section in the file. Used by NetWitness for integrity check. For example, `"Checksum": "883DACF97E4BCD9F590A1461A4DD0A312B5883A6CF82E0518E77AAB6A6DDB654"`

Example

Here is a sample JSON file.


```
{
    "Content": {
        "Components": [{
            "Version": "11.3.0.0",
            "Id": 7,
            "Properties": [{
                "Value": "57470c96e4b0cf62c7bfbd53",
                "Name": "InstanceId"
            }],
            "Name": "esa"
        },
        {
            "Version": "11.3.0.0",
            "Id": 4,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e69",
                "Name": "InstanceId"
            }],
            "Name": "incidentmanagement"
        },
        {
            "Version": "11.3.0.0",
            "Id": 2,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e65",
                "Name": "InstanceId"
            }],
            "Name": "sa"
        },
        {
            "Version": "11.3.0.0",
            "Id": 1,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e63",
                "Name": "InstanceId"
            }],
            "Name": "malwareanalysis"
        },
        {
            "Version": "11.3.0.0",
            "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"
}
```


The JSON file includes details of all the licenses currently available on the appliance. Here is a sample of the Entitlement information within the JSON file for a appliance license for Broker.

```
    }, {
        "Version": "2015.0506",
        "Id": 14,
        "Properties": [{
            "Value": "M133206102",
            "Name": "SerialNumber"
        }, {
            "Value": "Broker",
            "Name": "DeviceType"
        }, {
            "Value": "PERPETUAL",
            "Name": "FeatureType"
        }, {
            "Value": "-1",
            "Name": "Threshold"
        }, {
            "Value": "1000654868",
            "Name": "AccountId"
        }, {
            "Value": "B02E-03A1-08A6-EC3B",
            "Name": "ActivationId"
        }, {
            "Value": "2015-05-05 00:00:00",
            "Name": "LicenseStartDate"
        }, {
            "Value": "permanent",
            "Name": "LicenseEndDate"
        }, {
            "Value": "20t-52osb7",
            "Name": "FeatureId"
        }, {
            "Value": "smcBroker",
            "Name": "Name"
        }, {
            "Value": "20t-52osb7",
            "Name": "InstanceId"
        }],
        "Name": "Entitlement"
    }, {
```


Upload Data to NetWitness for Live Feedback

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

If the Live Account is not configured, you can manually upload the usage data to NetWitness. 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 NetWitness.

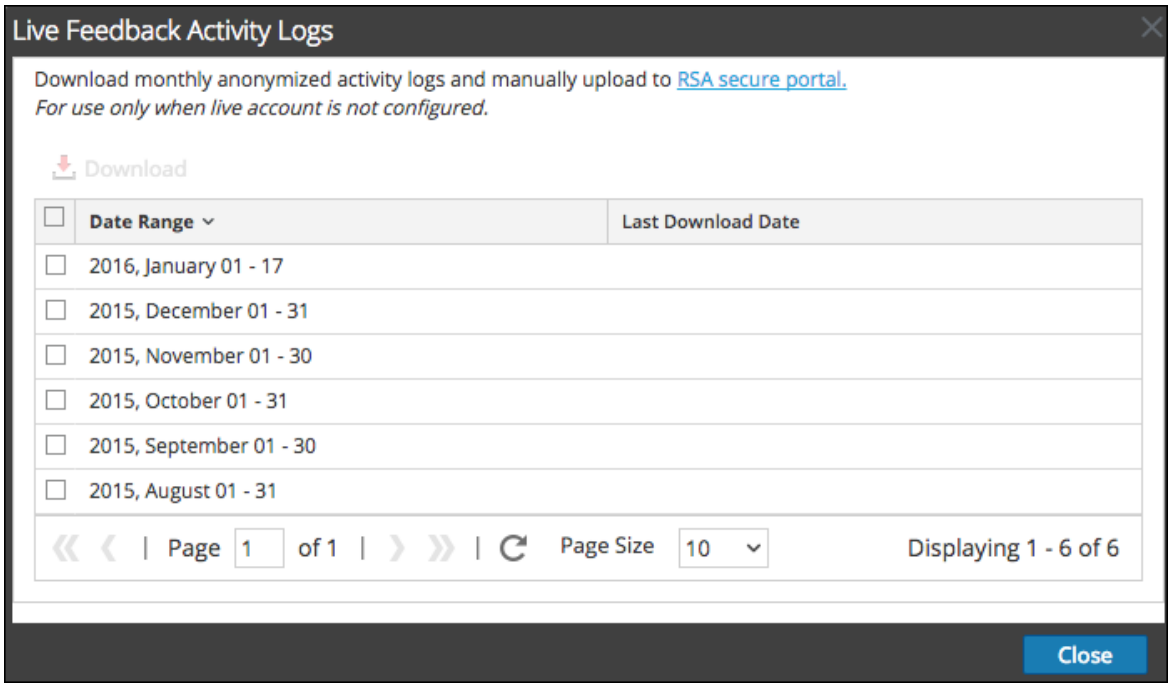
Download Live Feedback Historical Data

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 **Live Feedback Activity Log**.

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



4. Select one or multiple entries by setting 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.

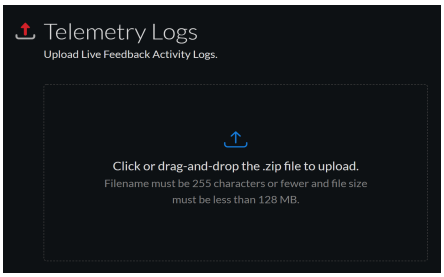
Share Data with NetWitness

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

Note:
- To download the Live Feedback data, see topic Download Live Feedback Historical Data.
- You can share data using the new live registration portal. For more information, Create Live Account.

To share the data to NetWitness

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



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

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

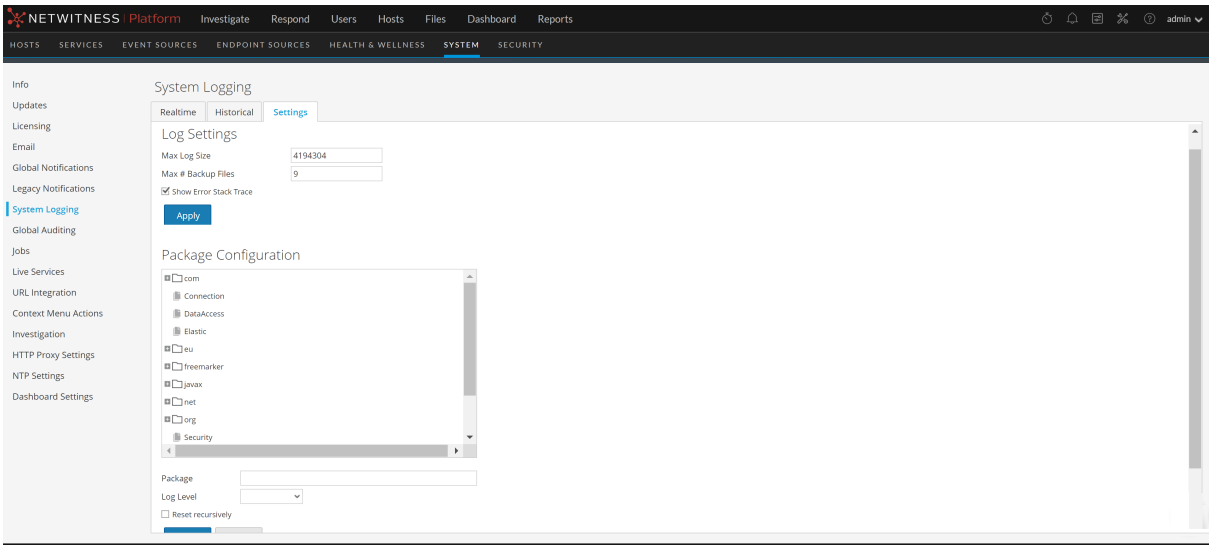
Configure Log File Settings

In NetWitness Platform, 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.

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.



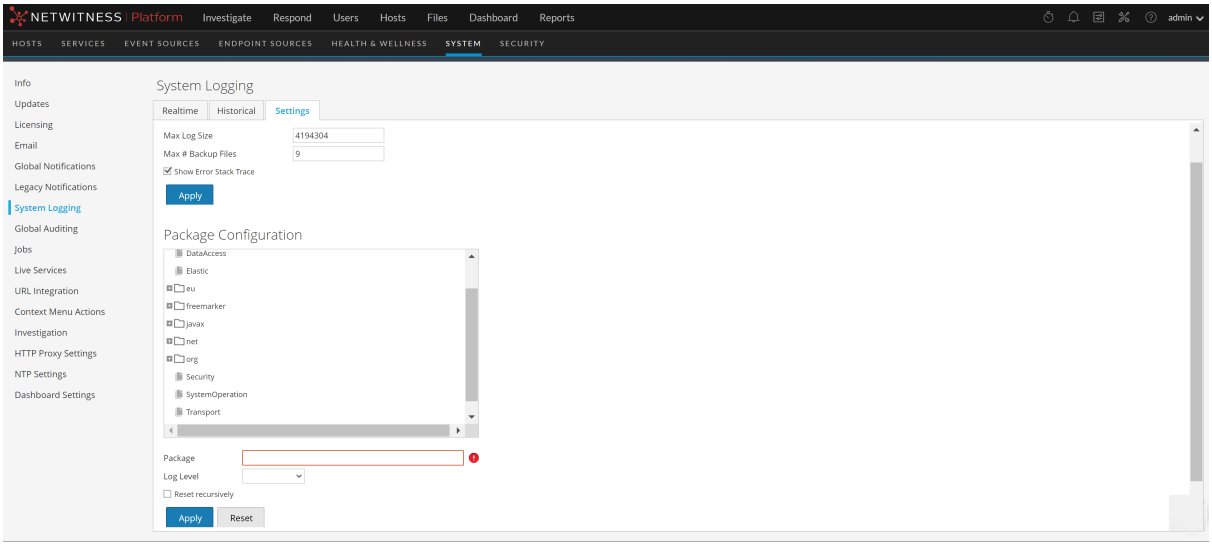
3. Click the **Settings** tab.
4. In the **Max Log Size** field, type the maximum size in bytes. The minimum value for this setting is **4096**.
5. In the **Max # Backup Files** field, type the maximum number of backup logs to maintain. The minimum value for this setting is **0**. When the maximum number 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 Network in a tree structure. The tree contains all the packages used within NetWitness. 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**.

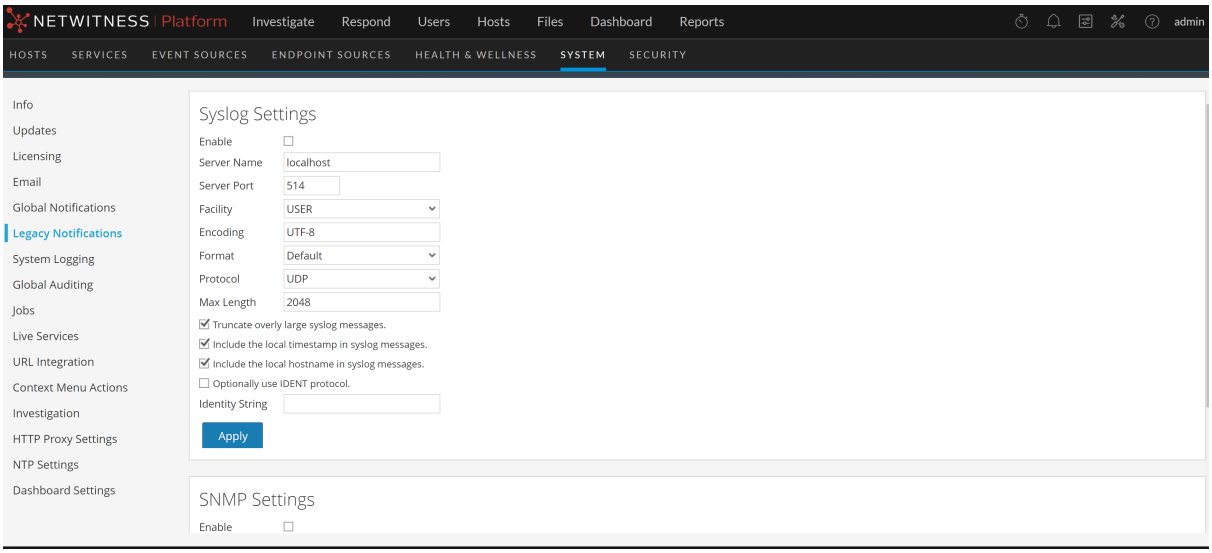
Configure Syslog and SNMP Settings

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**.
2. In the options panel, select **Legacy Notifications**.

   The Legacy Notifications Configuration panel is displayed.



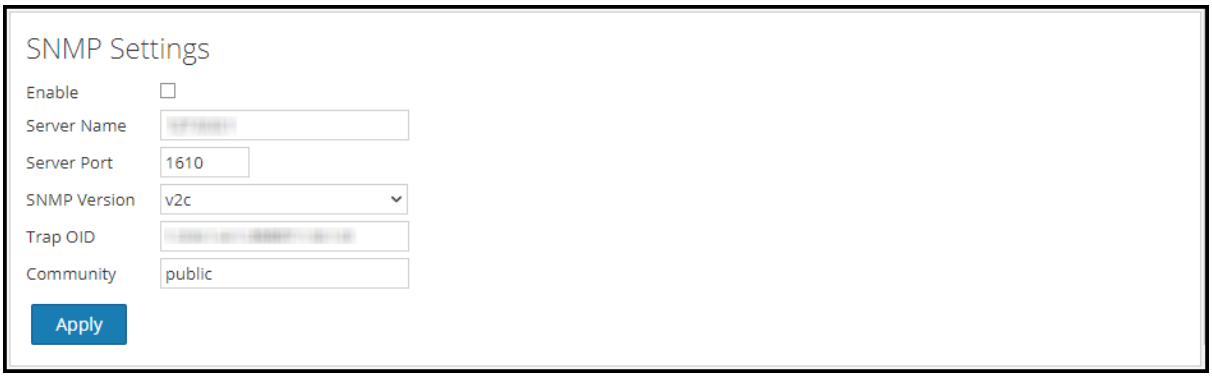
3. In the **Server Name** and **Server Port** fields under **Syslog Settings**, type the host name where the target syslog process is running and the port where the target syslog process is listening.
4. In the **Facility**, **Encoding**, **Format**, and **Max length** fields, specify the syslog facility, message text encoding, message format, and maximum message length.
5. In the **Protocol** field, select either UDP or TCP.
6. (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**.
7. (Optional) Configure syslog to prepend an Identity String before each syslog alert.
8. Set the **Enable** checkbox.
9. Click **Apply**.

Syslog notifications are immediately enabled. Legacy Notifications Configuration Panel provides detailed information about these settings.

Configure and Enable SNMP Settings

1. Go to **(Admin) > System**.
2. 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 **0.0.0.0.0.1**.
6. In the **Community** field, specify the community string used to authenticate on the SNMP trap host, the default value is **public**.
7. Set 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 instance:

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

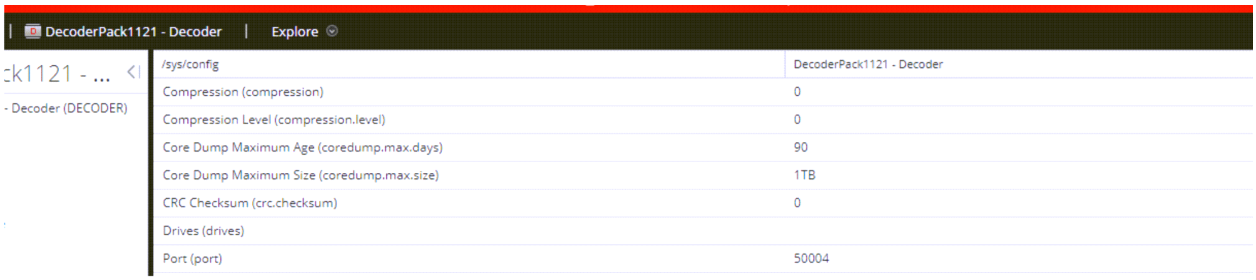
Additional Procedures

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

Configure Core Dump Retention

When a NetWitness service starts, it checks the cores directory for core files. If any are older than 90 days, they are deleted. Then, if the core files take up more than 500 GB, the service will delete them from the oldest until the core files are under this limit.

From 12.3 and later, a new feature is added to all NetWitness services allowing the user to customize the time and size limits using new configuration parameters under the `/sys/config` node in the Explore view.



This picture shows the new parameters in the explore screen on a decoder. To update, simply click the value and enter a new value as you would with any other configuration parameter. The new values will take effect the next time the service starts.

Parameters

- Core Dump Maximum Age
- Core Dump Maximum Size

Core Dump Maximum Age

This parameter controls the maximum number of days that the service will keep core files. Any core file older than the number shown here (in days) will be deleted when the service starts. The default is 90. The values range from 10 to 1825 (5 years)

Core Dump Maximum Size

This parameter controls the maximum number of bytes that core files can take on the disk. When the service starts, if the total of all core files is over this limit, the service will start deleting files starting with the oldest until the total amount of disk space used is under this limit. The default is 500 GB, and the range is 10 GB -1000000000 GB. "0" is allowed and means unlimited.

Caution: As the core files are kept on the same drive as the meta DB. As such, the value for Core Dump Max Size should be coordinated with the meta DB space limitations and the physical storage size.

Configure Proxy for NetWitness Platform

This topic provides a procedure for setting up a proxy that is used across NetWitness modules and services.

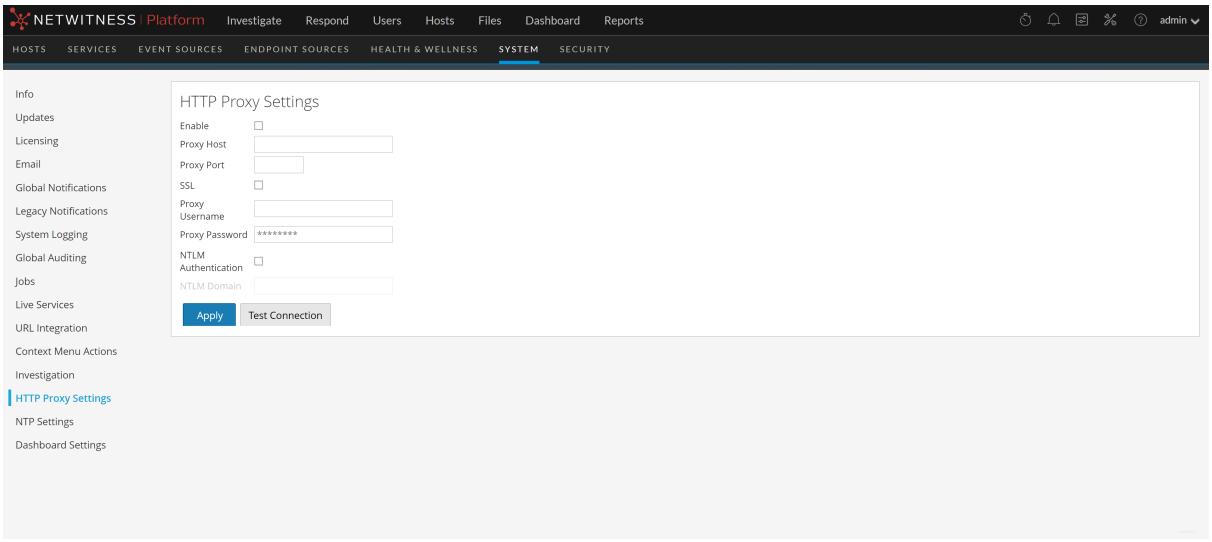
Note: Proxy support is only for HTTP and HTTPS proxies and not SOCKS5.

You can configure a proxy that is used across NetWitness modules and services in the System View > Advance Configuration panel. The Proxy Settings in the Advanced Configuration panel set up a proxy to be used wherever a proxy is needed in NetWitness. These settings override any proxy settings configured for an individual service or module, such as Malware Analysis or Live.

To configure a proxy for use across NetWitness modules:

1. Go to  **(Admin) > System**.
2. In the options panel, select **HTTP Proxy Settings**.

   The HTTP Proxy Settings panel is displayed.



3. Click the **Enable** checkbox.

   The fields where you configure the proxy settings are activated.

4. Type the hostname for the proxy server and the port used for communications on the proxy server.
5. (Optional) Type the username and password that serve as credentials to access the proxy server if authentication is required.
6. (Optional) Enable **Use NTLM Authentication** and type the NTLM domain name.
7. (Optional) Enable **Use SSL** if communications use Secure Socket Layer. If you enable **Use SSL**, ensure that you import the required certificates for the services to retrieve information.

   You need to import certificates and add the certificate in the head node for all the specific services that communicate externally over a proxy. If there are any other service that communicates with external resources over the internet, ensure that you add the certificates. For more on how to add the certificates, see Import Certificates for HTTPS Service
8. The proxy is immediately available for use throughout NetWitness modules and services, for example, Live and Malware Analysis.
9. To save and apply the configuration, click **Apply**.

Import Certificates for HTTPS Service

Import certificates to communicate with the HTTPS services:

1. SSH to the NW node and copy the CA certificate located in the following directory:
   /etc/pki/ca-trust/source/
2. Execute the following command to update the certificates:
   `update-ca-trust`
3. Execute the following command to add the certificate to the java keystore:
   `keytool -list -keystore /etc/pki/java/cacerts -storepass changeit |& head`
4. Restart the service on the NW node.

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

Add Custom Context Menu Actions

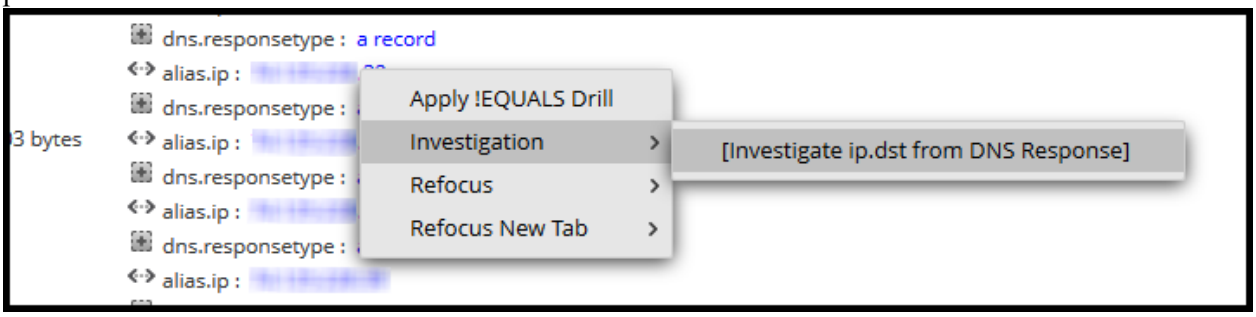
In the Context Menu Actions panel, Data Privacy Officer, Administrator, Analyst, and SOC Manager can view, add, edit, delete, import, and export context menu actions for the current instance of NetWitness. Each context menu action applies to a specific context in the NetWitness user interface, and appears as an option when you right-click a specific location in the user interface.

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. To copy, switch to the Advanced view, open the action and copy the JSON configuration file, create a new action/edit an existing action and paste. A context menu action is defined by:

- Action: The title of the action in the context menu.
- Component: The NetWitness module in which the context menu is available.
- Meta key: The content to which the action applies.
- Definition: The definition of the action.

Note: All context menu actions created before you upgrade to 11.3, functions as configured.

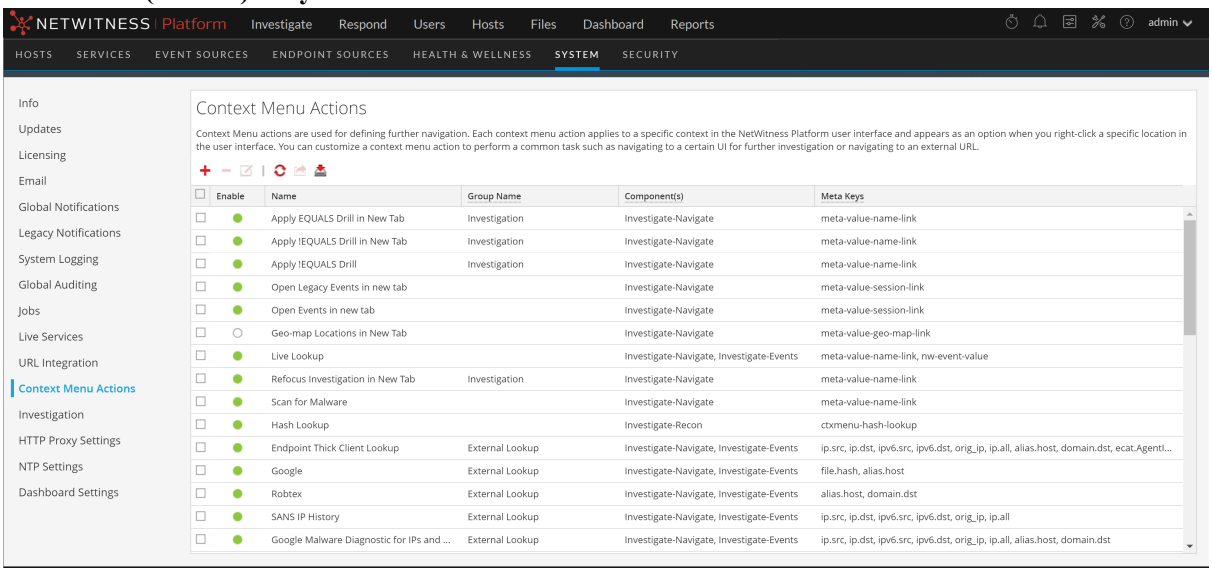
This is an example of a custom context menu action; the steps to create this example are provided as a procedure below.



View Context Menu Actions in NetWitness

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

1. Go to  **(Admin) > System.**

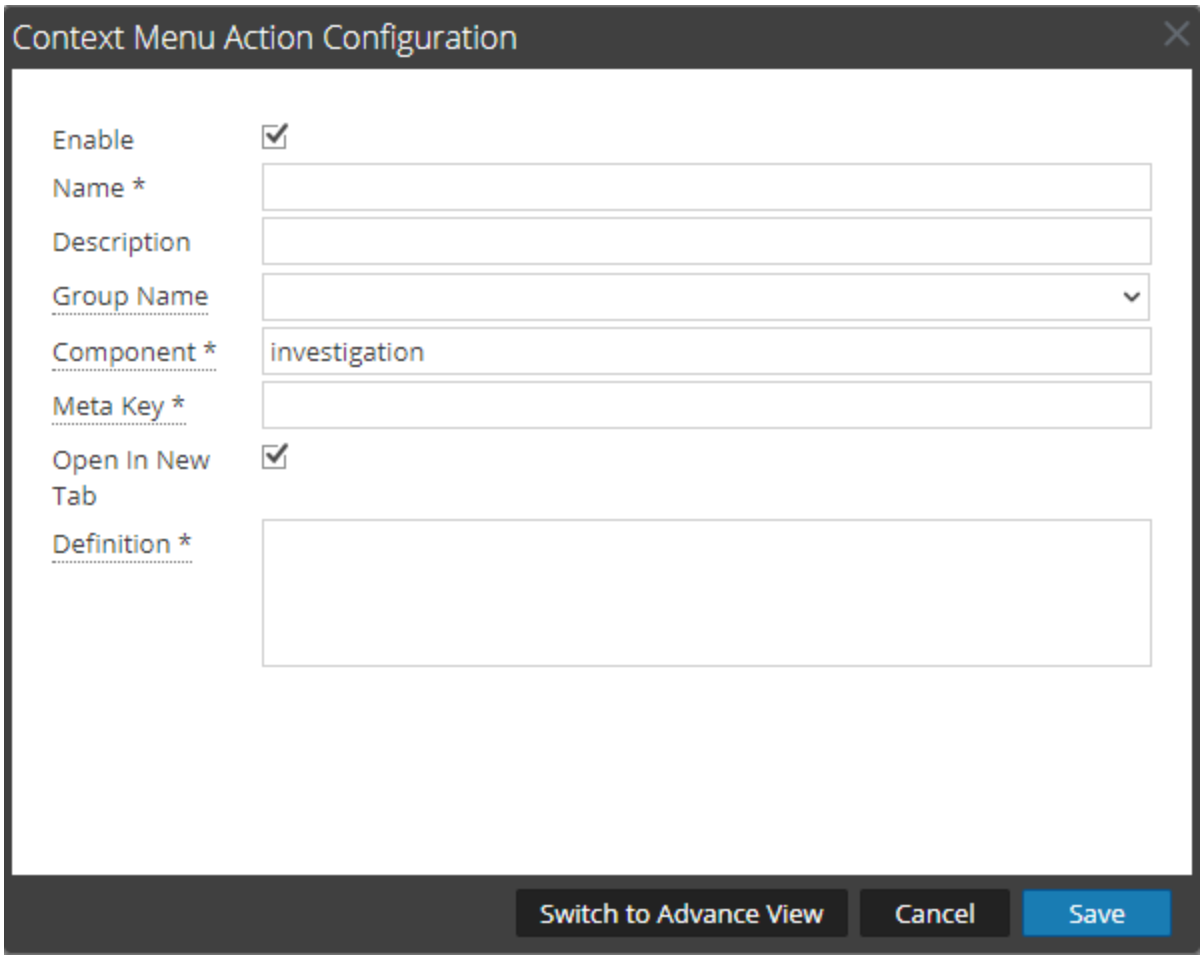


2. In the options panel, select **Context Menu Actions**.
   All the new actions which were available in NetWitness Suite 11.1 in the Investigate > Events tab can now be configured using the context menu actions. Details of the information in the Context Menu Action panel are provided in Context Menu Actions Panel.

Add a Context Menu Action

To add a context menu action in NetWitness:

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



Fill the required fields:

a. Enable: Select Enable to enable this context menu action.

b. Name: Enter the name of the context menu action.

c. Description: Enter a description of the context menu action.

d. Group Name: Select the group name from the drop-down menu. The action appears under this group in Context menu.

e. Component: The name of the component under which action will appear in the user interface. For example. under Investigate, the Context menu action can appear under Investigate-Navigate, Investigate-Legacy Events, Investigate-Event Recon and Investigate-Events.

Note: The Investigate-Legacy Events option and related data is displayed only if the Enable Legacy Events checkbox is enabled under **(Admin)** > **System** > **Investigation** > **Legacy Events**.

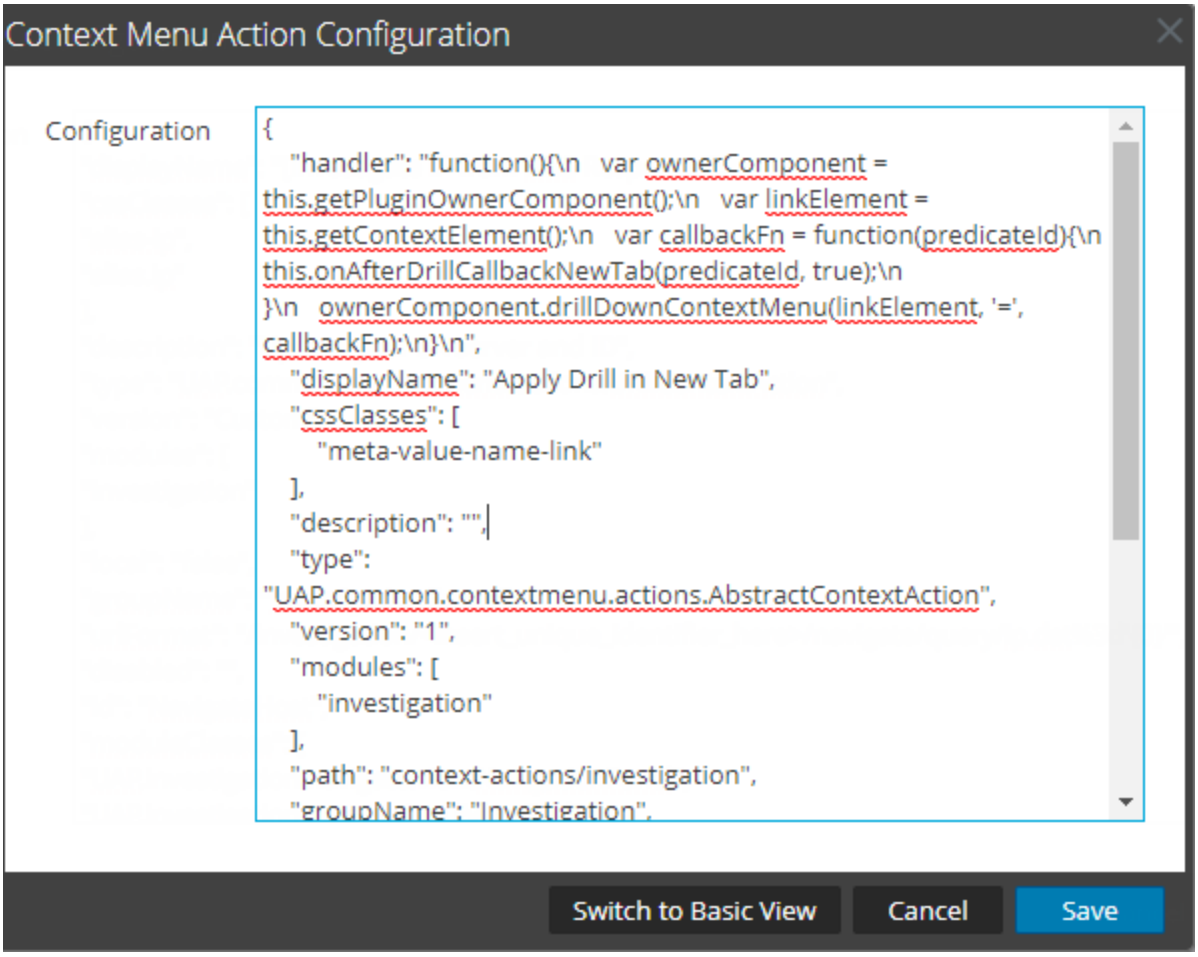
f. Meta Key: Enter the meta key separated by commas to further narrow-down scope for the context menu action. The action will appear on these meta key. Context menu actions have to be defined specifically for each meta key, the key references in a meta key do not inherit a context menu actions. For example, a context menu action created for ip.all are not created for ip.src as well. A

separate action has to be created for the sub-category or key reference of a meta.

g. Open in New Tab: Select this option to open the context menu action in a new tab.

h. Definition: Enter further action performed for this context menu action. For example, open a certain user interface or navigate to an external URL.

2. You can also 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. Click **Switch to Advance View** to add the context menu action.



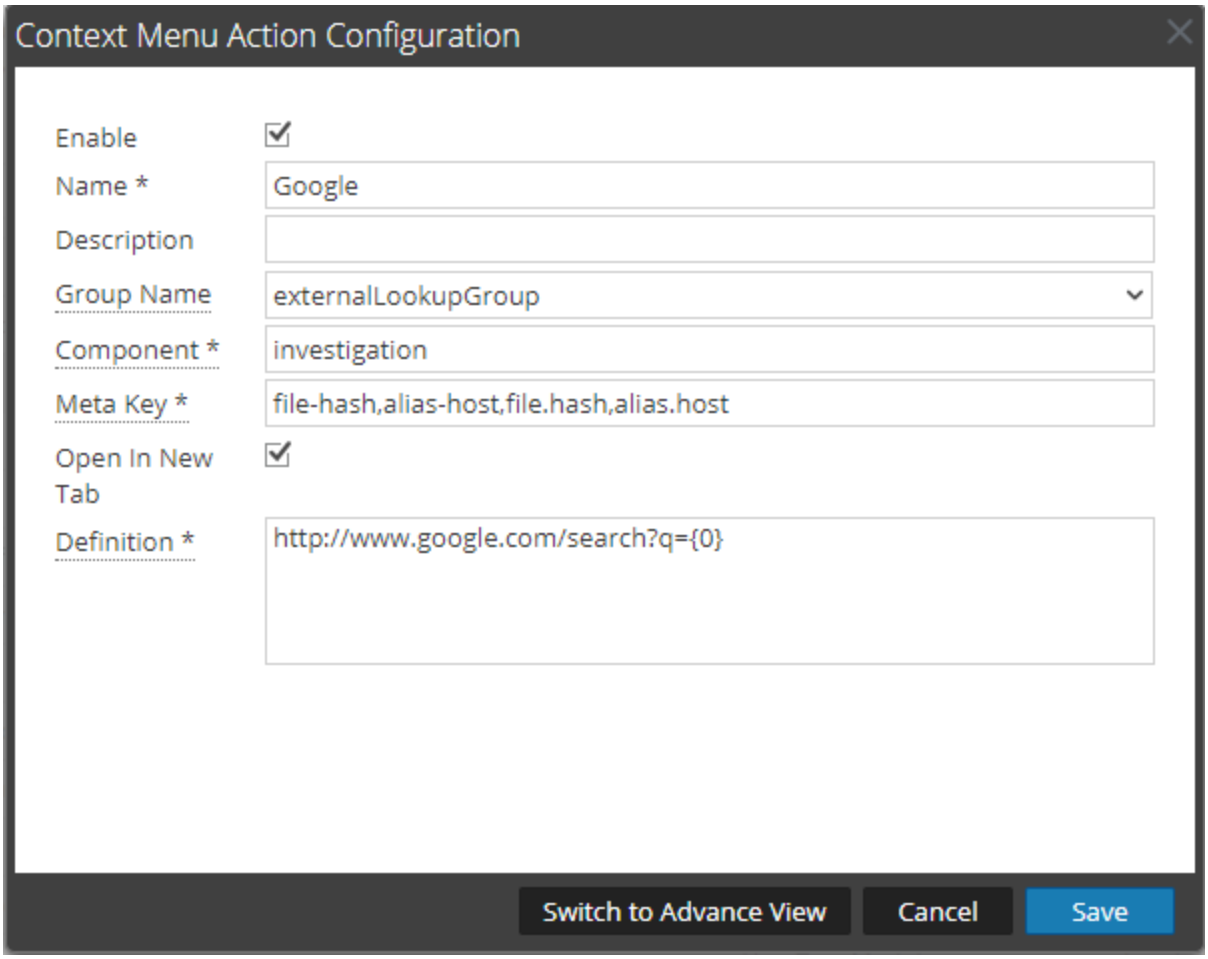
3. Click **OK.**
The new context menu action is created and added at the end of the list of context menu actions.

4. The context menu action becomes available in the configured location.

Edit a Context Action

To edit a context action:

1. Select the row in the grid and either **double-click** the row or click  .
The **Context Menu Action Configuration Dialog** is displayed.



2. Edit the **Configuration**.
3. To save the changes, click **OK**.

Delete a Context Action

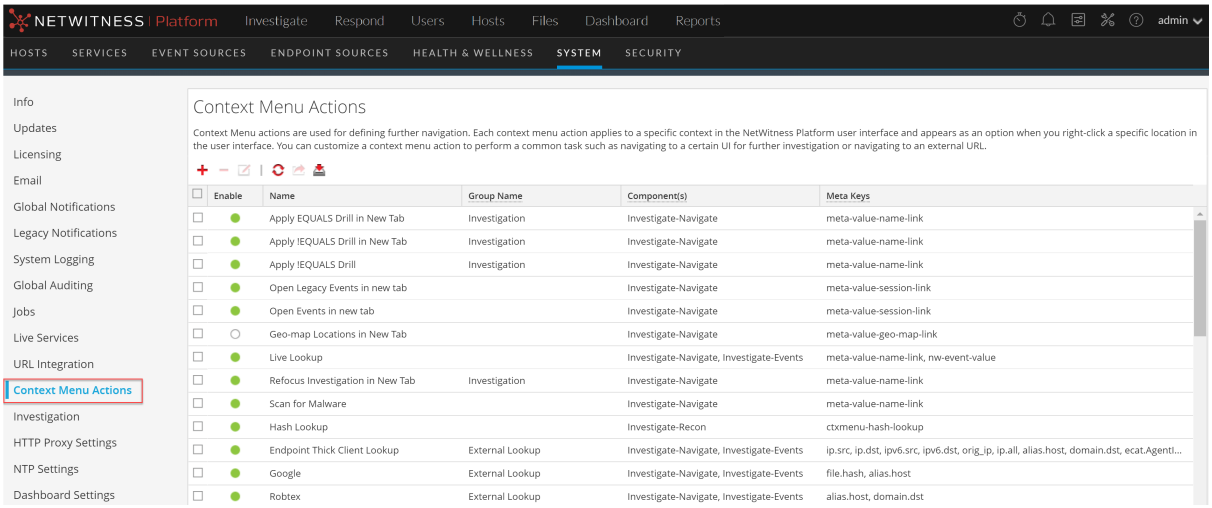
To remove a context menu action from NetWitness entirely:

1. Select the action.
2. Click .
   A dialog requests confirmation that you want to delete the context menu action.
3. Click **Yes**.
   The option is removed from the Context Menu Actions panel.

Export Context Menu Actions

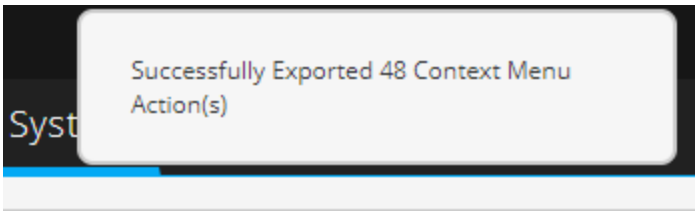
You can export context menu action to a zip file. The zip file contains the JSON files with each each JSON file mapping to a context menu action. To export the context menu action, follow these steps:

1. Go to **(Admin) > System**.
2. Click **Context Menu Actions**.



3. Click to select a context menu action to import. Click the header to select ALL the context menu actions.

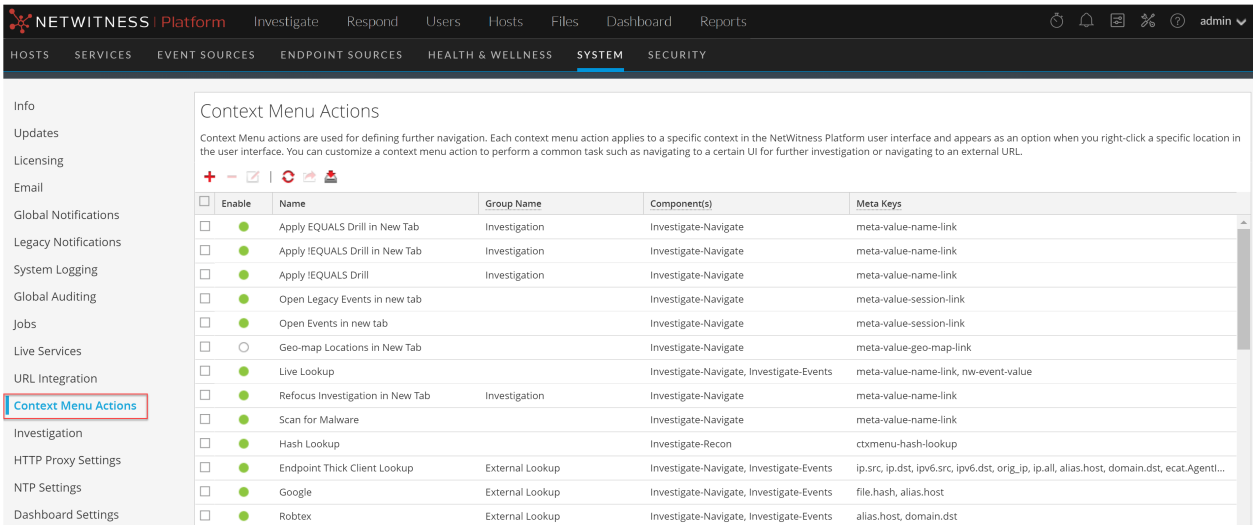
4. Click Export Action(s) under Context Menu Actions.
5. The success message confirming the actions uploaded successfully is displayed.



Import Context Menu Actions

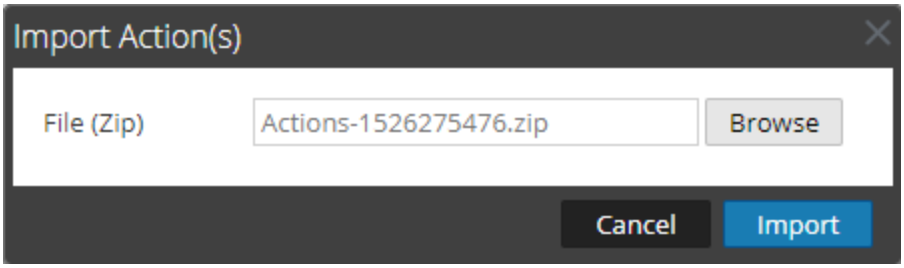
You can import context actions in Context Menu Actions tab. These actions can then be edited or used as is for investigating context where applicable. Follow these steps to import a context menu action(s):

1. Go to **(Admin) > System**.
2. Click **Context Menu Actions**.



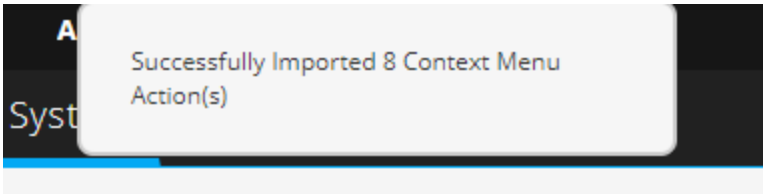
3. Click Import Action under Context Menu Actions.
4. In Import Action click **Browse** to locate and select the file. The zip file typically contains the json files containing context menu actions exported previously.

5. Select the Zip file and click **Open**.
6. Click **Import**



Note: There is no validation for an action for Events with a Javascript function.

7. The success message confirming the actions uploaded successfully are displayed.



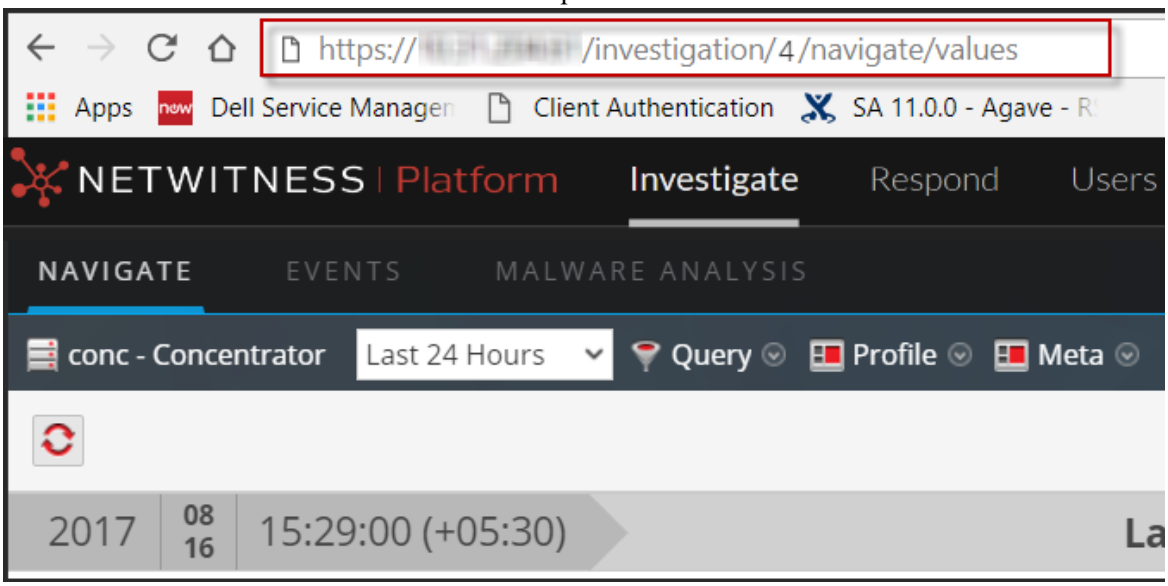
Note: If an error message is displayed, check the log files and try importing the context menu actions file again.

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.

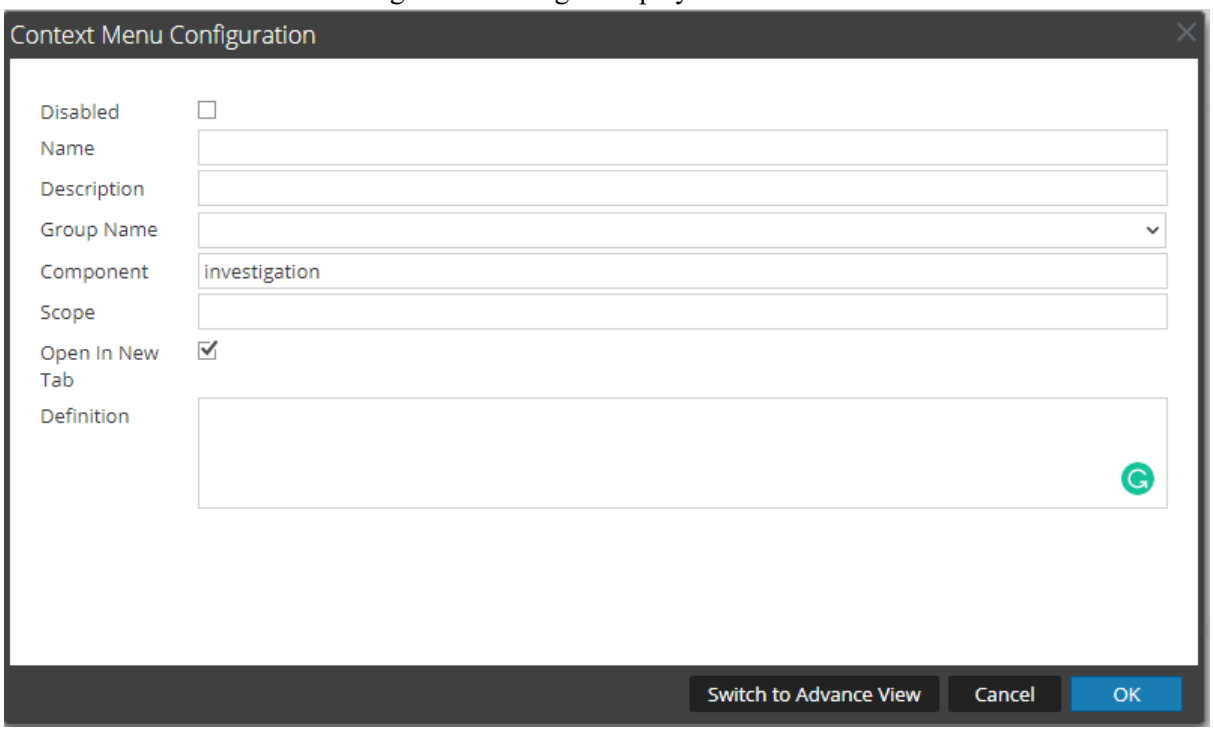
To implement the context menu action:

1. Determine the unique identifier for your NetWitness Server as follows:
   a. Log onto NetWitness , go to **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.



2. Go to  **(Admin) > System > Context Menu Actions**
   In the toolbar, click  .

The Context Menu Action Configuration dialog is displayed.

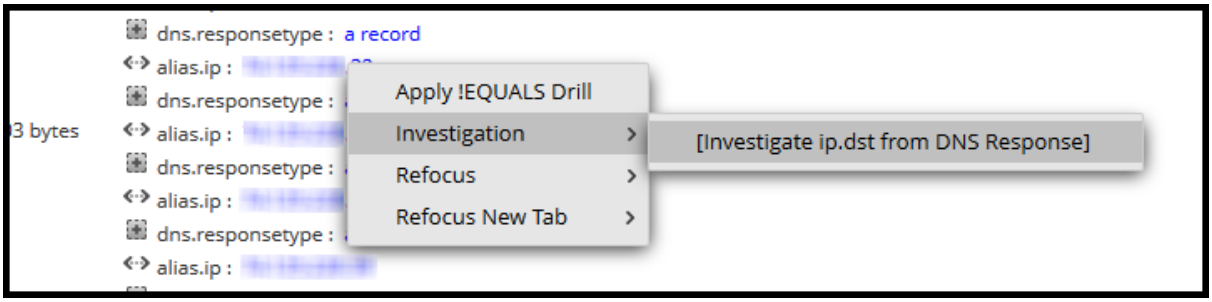


3. Copy the entire sample code block below and paste it in the window.

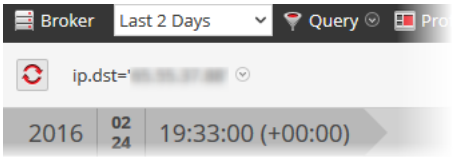
```
{
    "displayName": "[Investigate IP from DNS Response]",
    "cssClasses": [
        "alias-ip",
        "alias.ip"
    ],
    "description": "Update your NW server and ID",
    "type": "UAP.common.contextmenu.actions.URLContextAction",
    "version": "Custom",
    "modules": [
        "investigation"
    ],
    "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"
}
```

4. 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}'"`
5. Click **OK**, and restart your browser.
6. 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.



7. Should produce a pivot like this.



8. 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 *NetWitness Investigate 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: NetWitness Server Core hosts must be able to communicate with the NetWitness Server host with UDP port 123 for NTP time synchronization.

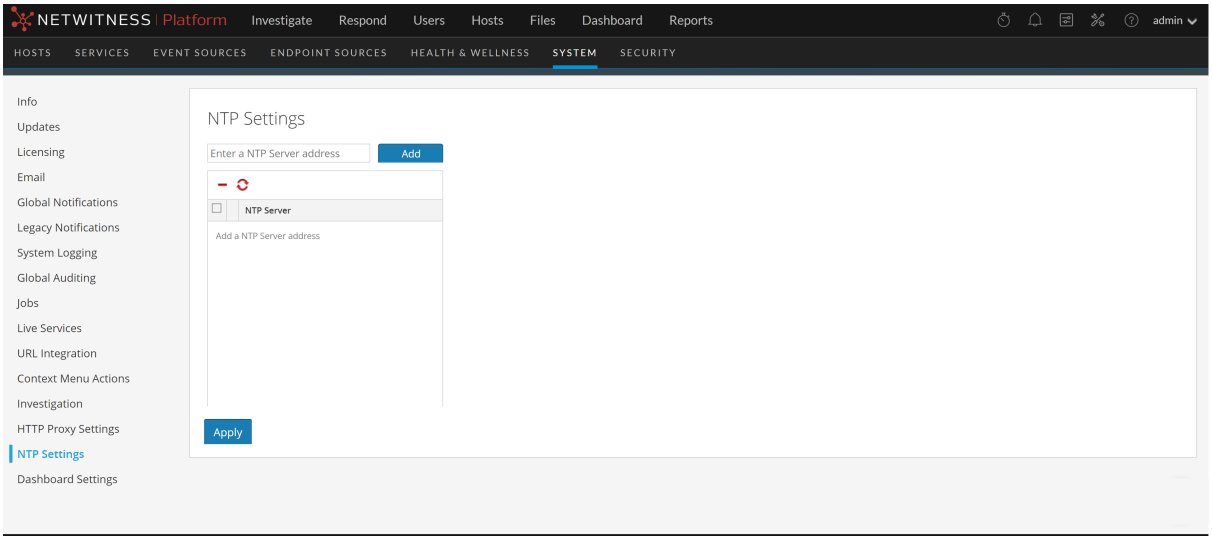
You use the **(Admin)** > **System** > **NTP Settings** view to configure one or more NTP servers. After you configure an NTP server, NetWitness uses NTP to synchronize the host machine clocks. You configure multiple NTP servers for Fail Over purposes. This topic contains the following procedures:

- 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.



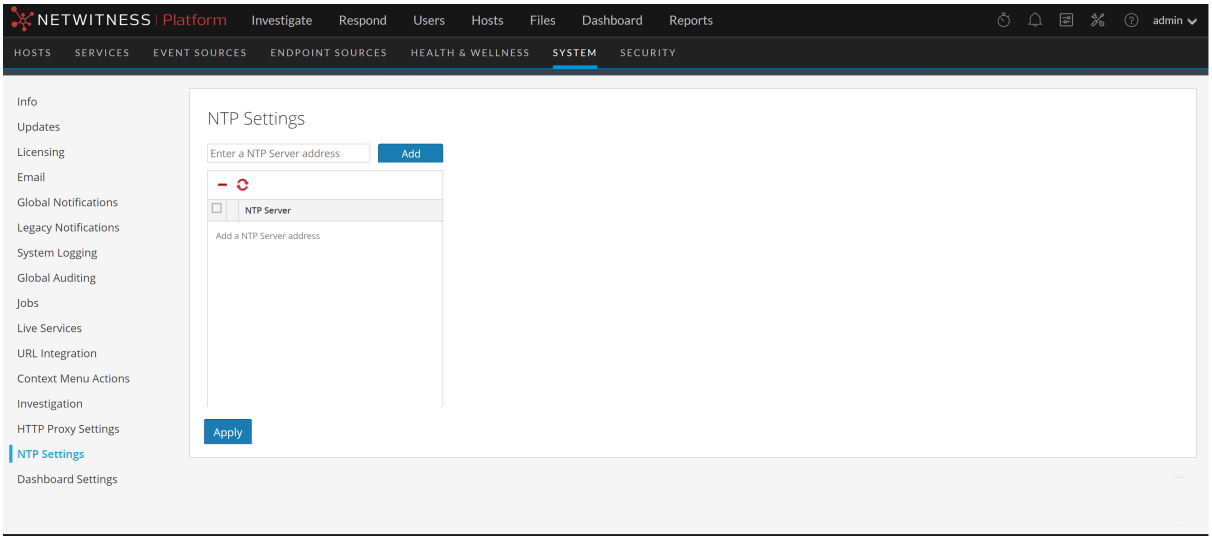
3. Enter the IP address or FQDN for an NTP server.
   If the hostname syntax is invalid, NetWitness disables the **Add** and **Apply** buttons and displays **Entered an invalid hostname**.
4. Click **Add**.
   - If the hostname syntax is valid and NetWitness can reach the server, it displays **Validating**.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

For details of the parameters and descriptions, see NTP Settings Panel.

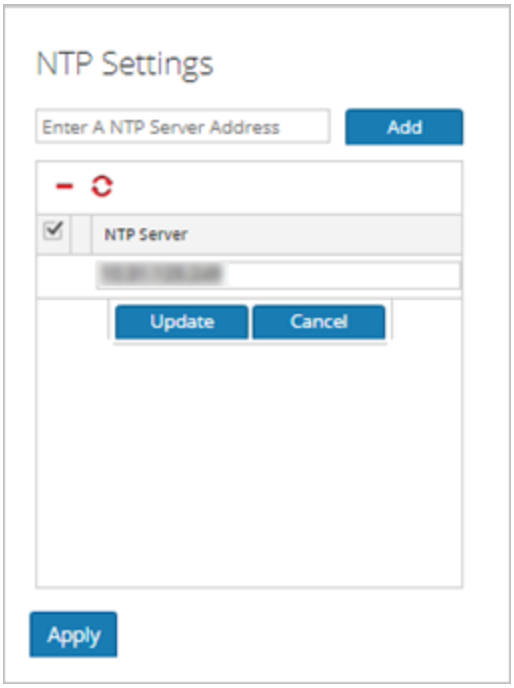
Modify an NTP Server

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.



4. Edit the hostname, click **Update**, and click **Apply.** (click **Cancel** before you click **Apply** to cancel the edit.)
   NetWitness changes the hostname according to your edits.

Troubleshoot System Configuration

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

- Troubleshoot Global Audit Logging
- Troubleshoot Issues identified in the NTP Settings Panel or Log Files Messages
- Troubleshoot Global Notifications

Troubleshoot Global Audit Logging

This topic provides information about possible issues that NetWitness users may encounter when implementing Global Audit Logging in NetWitness. 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 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 Server host aggregates audit logs from all of the NetWitness services, coverts 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 user interface.

Define a Global Audit Logging Configuration provides instructions.

Verify the Packages and Services on the Hosts

NetWitness Host

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

- rsyslog-8.4.1
- rsa-audit-rt
- logstash-5.6.4
- rsa-audit-plugins
- rabbitmq server

Services on a Host other than the NetWitness Host

The following packages or services must be present on each of the NetWitness 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

A service is not logging to the local syslog server.	• Ensure that rsyslog is up and running. You could use the following command:
	`service rsyslog status`
	• Ensure that rsyslog is listening on port 50514 using UDP.
	You could use the following command:
	`netstat -tulnp|grep rsyslog`
	• 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:
	`sudo tcpdump -i lo -A udp and port 50514`
	See "Solution Examples" below to view the command outputs.

Audit logs are not getting uploaded to RabbitMQ from the local syslog.	• Ensure that the rsyslog plugin is up and running. You could use the following command:
	`ps -ef|grep rsa_audit_onramp`
	• Ensure the RabbitMQ server is up and running.
	You could use the following command:
	`service rabbitmq-server status`
	See "Solution Examples" to view the command outputs.

Audit logs are not aggregated on the NetWitness Server host.	• Ensure Logstash is up and running. You could use the following commands:
	`ps -ef|grep logstash`
	`service logstash status`
	• Ensure the RabbitMQ server is up and running.
	You could use the following command:
	`service rabbitmq-server status`
	• Ensure the RabbitMQ server is listening on port 5672.

Issue	Possible Solutions

	You could use the following command:
	`netstat -tulnp|grep 5672`
	• Check for any errors generated at the Logstash level.
	You could use the following command for the location of the log files:
	`ls -l /var/log/logstash/logstash.*`
	See "Solution Examples" to view the command outputs.

Aggregated logs on the NetWitness Server host are not being forwarded to the configured third-party syslog server or Log Decoder.	• Ensure Logstash is up and running.
	You could use the following commands:
	`ps -ef|grep logstash`
	`service logstash status`
	• Check for any errors generated at the Logstash level.
	You could type the following command for the location of the log files:
	`ls -l /var/log/logstash/logstash*`
	See "Solution Examples" below to view the command outputs.
	• Ensure that the destination service is up and running.
	• Ensure that the destination service is listening on the correct port using the correct protocol.
	• Ensure that the configured port on the destination host is not blocked.

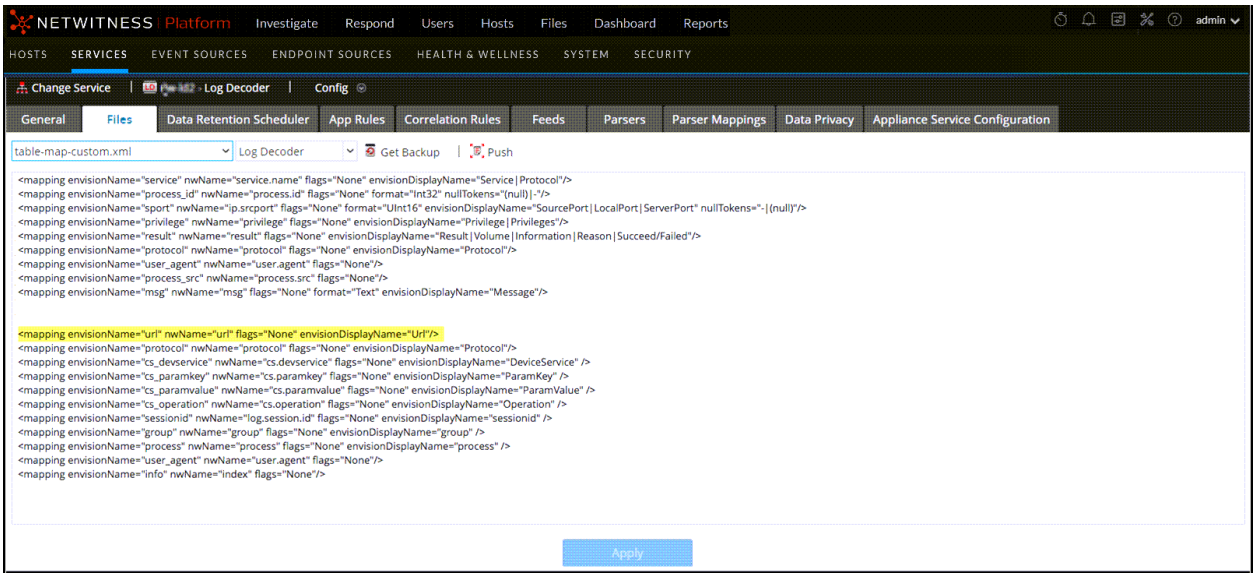
Audit logs forwarded from the Logstash lead to parse failure at the Log Decoder.	• Ensure that you are using an appropriate notification template. Audit Logs parsed by a Log Decoder must be in CEF format. The destination from which audit logs directly or indirectly make their way to the Log Decoder must also use a CEF Template. • 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. Define a Template for Global Audit Logging provides additional information. • Verify the Logstash configuration.

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.

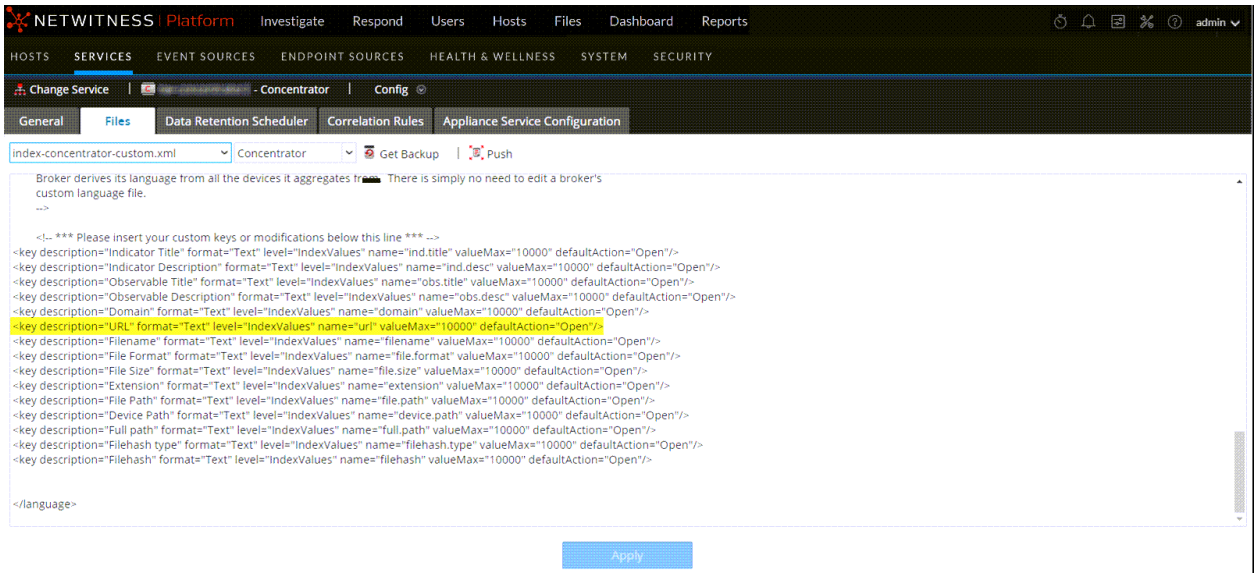


The `url` custom meta example is highlighted in the following code sample from the **table-map-custom.xml** file above:

```
<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..m..@.@.:~..........R.Y.m<38>2015-04-24T08:54:46Z NWAPPLIANCE22574 SA_SERVER {"category":"DATA_ACCESS","deviceProduct":"Security Analytics","deviceService":"SA_SERVER","devic
eVendor":"RSA","deviceVersion":"10.5.0.0","identity":"Unknown identity","operation":"/poll/cda459a3-4e9d-ce1f-20f2-8cb1e31ef198","outcome":"Success","parameters":"{referrer=http
s://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, queryStrin
g=ctoken=b33b67c5-6ae9-47b4-b435-560ecd38b760, remoteAddress=10.30.97.119}","severity":6}

08:54:46.615748 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","devic
eVendor":"RSA","deviceVersion":"10.5.0.0","identity":"admin","key":"user.general.contextmenu","operation":"Users.preferences.","severity":6,"userRole":"Administrators+Administra
tors+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","devic
eVendor":"RSA","deviceVersion":"10.5.0.0","identity":"admin","key":"user.notifications.enabled","operation":"Users.preferences.","severity":6,"userRole":"Administrators+Administ
rators+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","devic
eVendor":"RSA","deviceVersion":"10.5.0.0","identity":"admin","key":"user.browser_timezone_zoneId","operation":"Users.preferences.","severity":6,"userRole":"Administrators+Admini
strators+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","devic
eVendor":"RSA","deviceVersion":"10.5.0.0","identity":"admin","key":"user.browser_timezone_zoneId","operation":"Users.preferences.","severity":6,"userRole":"Administrators+Admini
strators+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,"INETS  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:C
MSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -jar /opt/logstash/vendor/jar/jruby-complete-1.7.11.jar -I/opt/logstash/lib /opt/logstash/lib/logstash/runner
.rb agent --pluginpath /opt/logstash -f /etc/logstash/conf.d -l /var/log/logstash/logstash.log
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.

Troubleshoot Issues identified in the NTP Settings Panel or Log Files Messages

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

Issue	Possible Solutions
Message	User Interface: **Unexpected error occurred. First check the logs then contact Customer Care to resolve error.** **System Log:** **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
Possible Cause	Low level NetWitness configuration is in error or supporting service is not running.
Solution	Contact Customer Care.
Message	User Interface: **Specified an invalid Hostname syntax**.
Possible Cause	Tried to enter NTP server hostname that does not confirm to IP address or FQDN syntax.
Solution	Reenter hostname in using correct syntax.
Message	User Interface: **Specified NTP server that already exists.**
Possible Cause	Tried to enter NTP server hostname that is already defined in NetWitness.
Solution	Enter hostname for an NTP server not configured in NetWitness.
Message	User Interface: **Cannot reach NTP server *hostname***. Please verify the server address and your firewall settings.
Possible	The server address or firewall settings may be in error.

Issue	Possible Solutions
Cause	
Solution	Verify the server address and your firewall settings and correct them if required.

Troubleshoot Global Notifications

This topic provides information about possible issues that NetWitness users may encounter when implementing Global Notifications in NetWitness.

Issue	Possible Solution
We are not receiving notifications that were configured for a service, but the service log file does not show any errors.	For any notification-related troubleshooting, check the `integration-server log` file in addition to the log file of the service creating the notification. For example, when troubleshooting ESA rule notifications, check both the ESA Correlation service log files (`/var/log/netwitness/correlation-server/correlation-server.log`) AND the Integration-Server log files on the NetWitness Server (`/var/log/netwitness/integration-server/integration-server.log`). If the `integration-server.log` file shows a failure when the Integration-Server attempts to send a notification to the notification server, you should check the notification server configuration in the Global Notifications settings (**(Admin) > System > Global Notifications > Servers** tab).

References

This topic provides reference materials that describe the user interface for configuring system settings in NetWitness 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
- 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 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.	Configure a Destination to Receive Global Audit Logs
Administrator	Choose an Audit Logging template.	Define a Template for Global Audit Logging

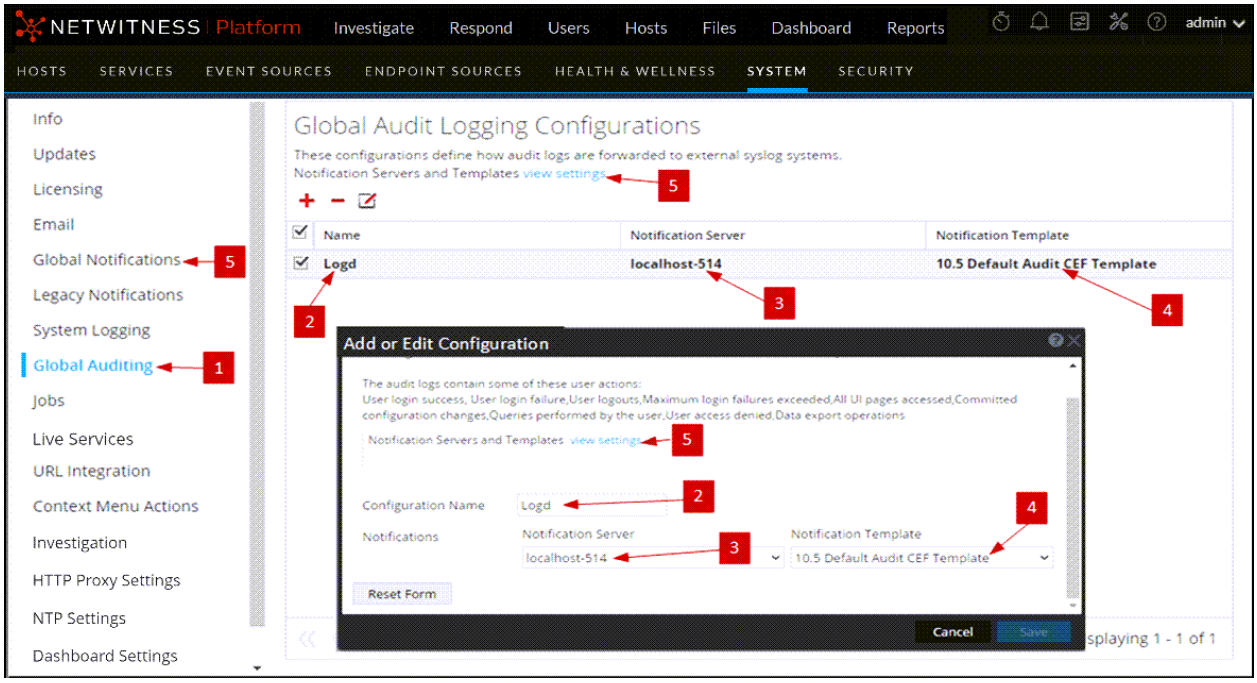
Role	I want to ...	Show me how
Administrator	Configure Global Audit Logging	Define a Global Audit Logging Configuration For the complete procedure, see "Global Audit Logging - High-Level Procedure" in Configure Global Audit Logging.
Administrator	Verify Global Audit logs	Verify Global Audit Logs

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 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 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.
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. Configure a Destination to Receive Global Audit Logs provides instructions on how to create a Syslog Notification Server for global audit logging.
Notification Template	Displays the Audit Logging Notification Template selected for the configuration. It defines the format and message fields of the audit log entries. For Log Decoders, 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 available CEF meta keys. 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 meta key variables.

Add New Configuration Dialog

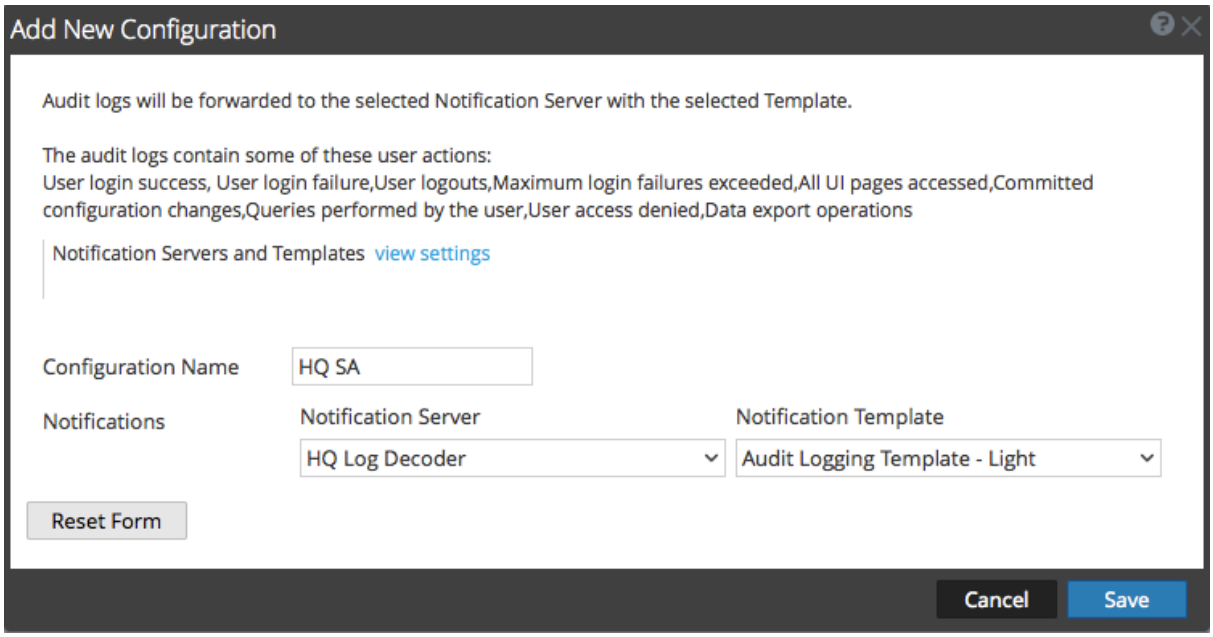
In the NetWitness Platform, Administration System view Global Audit Logging Configurations panel, you can create multiple global audit logging configurations. These configurations are used to forward global audit logs to a central location to perform user audits.

Procedures related to global audit logging are described in Configure Global Audit Logging.

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

1. Go to 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.



   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 **view settings** 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. Configure a Destination to Receive Global Audit Logs 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 **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. 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.
Reset Form 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. 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 (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`.

User Action	Example
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).

The following table shows examples of internal audit logs logged from NetWitness

User Actions	Audit Log Examples
User Login success	{"type":"fileclone","hostname":"UpdateStackAdminServer", "timegenerated":"2019-05-23T13:55:42.764124+00:00","syslogtag": "ADMIN-SERVER","@version":"1","fromhost-ip":"110.10.10.1”, "deviceVendor":"RSA","deviceService":"admin-server”, "deviceVersion":"11.3.1.0” “uri":"/oauth/token", "referrer":"https://10.111.201.10/login","success":"true", "identity":"AdminNorm","action":"Logon-Web","deviceServiceId": "247cedcb-cXXX-4XXX-8XXX-5XXXXa","deviceProduct":"NetWitness", "category":"Security","operation":"Logon-Web",”outcome": "success","remoteAddress":"101.181.15.10","message":null, "logTime":"2019-05-23T13:55:42.769Z","@timestamp":"2019-05 -23T13:55:42.769Z","timereported":"2019-05-23T13:55:42+00:00", "node_id":"e0XXX8-4XXX-4XXX-8XXXX-6d4b8XXXX09"}
User Login Failure	{"type":"fileclone","hostname":"UpdateStackAdminServer", "timegenerated":"2019-05-23T13:42:38.485701+00:00","syslogtag": "ADMIN-SERVER","@version":"1","fromhost-ip":"111.1.10.11", "deviceVendor":"RSA","deviceService":"adminserver","device Version":"11.3.1.0","uri":"/oauth/token","referrer":"https: //10.111.201.10/login","success":"false","identity":"AdminNor m", "reasonForFailure":"Bad Credentials","action":"Logon-Web", "deviceServiceId":"2XXXX-cXXX-4XXX-8XXX-5feXXXX2a","device Product":"NetWitness","category":"Security","operation": "Logon-Web","outcome":"failed","remoteAddress":"101.181.15.10", "message":null,"logTime":"2019-05- 23T13:42:38.494Z","@timestamp": "2019-05-23T13:42:38.494Z","timereported":"2019-05-23T13: 42:38+00:00","node_id":"e0XXXX-4XXX-4XXX-8XXX-6dXXXXX809"}

User Actions	Audit Log Examples
User Logouts	{"type":"fileclone","hostname":"UpdateStackAdminServer", "timegenerated":"2019-06-06T13:43:57.112760+00:00","syslogtag": "SOURCE-SERVER","@version":"1","fromhost-ip":"107.0.110.1,"device Vendor":"RSA","deviceService":"source-server","deviceVersion": "11.3.1.0","size":"0","success":"true","identity":"system", "action":"sourceCountUpdate","deviceServiceId":"c872d520-b06b-46cb-b5c1-8e240b105020","deviceProduct":"NetWitness","category": "SystemOperation","operation":"sourceCountUpdate","parameters": " {\"size\":\"0\"}","outcome":"success"},"message":null,"logTime" :"2019-06-06T13:43:57.117Z","@timestamp":"2019-06-06T13:43:57 .117Z","timereported":"2019-06-06T13:43:57+00:00","node_id": "e07b16f8-4xxx-4xx1-895b-6xxxxx09"}
All UI pages accessed	{"type":"fileclone","hostname":"UpdateStackAdminServer", "timegenerated":"2019-05-23T14:03:16.094611+00:00","syslogtag": "SA_SERVER","@version":"1","fromhost-ip":"117.10.10.11", "json": {"severity":"6","deviceVendor":"RSA","identity":"AdminNorm", "deviceService":"SA_ SERVER","deviceProduct":"NetWitness","device Version":"11.3.1.0","category":"DATA_ACCESS","userRole": "Administrators","operation":"HttpRequest",outcome":"Success"}, "message":null,"logTime":"2019-05-23T14:03:16.115Z","@timestamp": "2019-05-23T14:03:16.115Z","timereported":"2019-05-23T14:03:16Z", "node_id":"e0XXXX-4XXX-4XXX-8XXX-6d5XXXX09"} {"type":"fileclone","hostname":"UpdateStackAdminServer", "timegenerated":"2019-05-23T14:04:17.305585+00:00","syslogtag": "SA_SERVER","@version":"1","fromhost-ip":"117.10.10.1","json": {"severity":"6","deviceVendor":"RSA","identity":"AdminNorm", "deviceService":"SA_ SERVER","deviceProduct":"NetWitness","device Version":"11.3.1.0","category":"SYSTEM","userRole": "Administrators","operation":"Page Accessed","key":"[ADM] Hosts", "outcome":"Success"},"message":null,"logTime":"2019-05-23T14: 04:17.309Z","@timestamp":"2019-05-23T14:04:17.309Z","time reported":"2019-05-23T14:04:17Z","node_id":"e07XXXX-4XXX-4XXX-8XXX-6d55XXXXX09"}

User Actions	Audit Log Examples
Committed configuration changes	{"type":"fileclone","hostname":"UpdateStackAdminServer", "timegenerated":"2019-05-23T14:09:09.741982+00:00","syslogtag": "SA_SERVER","@version":"1","fromhost-ip":"117.101.0.11","json": {"severity":"6","deviceVendor":"RSA","deviceService":"SA_ SERVER" ,"deviceVersion":"11.3.1.0","identity":"AdminNorm","device Product":"NetWitness","category":"CONFIGURATION","userRole": "Administrators","operation":"Modified","parameters":"save", "value":"[10.10.201.10]","key":"ntp-servers","outcome":"Success"}, "message":null,"logTime":"2019-05-23T14:09:09.748Z","@timestamp": "2019-05-23T14:09:09.748Z","timereported":"2019-05-23T14:09:09Z", "node_id":"e07XXXX-4XXX-4XXX-8XXX-6dXXXXX9"}
Queries performed by the user	{"type":"fileclone","hostname":"UpdateStackAdminServer", "timegenerated":"2019-05-23T14:12:02.909062+00:00","syslogtag": "INVESTIGATE-SERVER","@version":"1","fromhost-ip":"117.10.10.11", "json":{"deviceVendor":"RSA","deviceService":"investigate-server","deviceVersion":"11.3.1.0*","success":"true","identity": "AdminNorm","action":"update","deviceServiceId":"f8XXXX5-bXXX-4XXX-bXXX-fXXXXX6","deviceProduct":"NetWitness","category": "Predicate","operation":"update","updated":"UserPredicateEntity (id=5cXXXXXXXXX9dd, userId=AdminNorm, predicateEntity=Predicate Entity(id=ff53, legacyId=null, query=user.all='solay', display Name=user.all='solay'), lastUsed=2019-05-23T14:12:02.897Z", "outcome":"success"},"message":null,"logTime":"2019-05-23T14:12:02.920Z","@timestamp":"2019-05-23T14:12:02.920Z","time reported":"2019-05-23T14:12:02+00:00","node_id": "e0XXXX-4XXX-4XXX-8XXX-6d5XXXXX09"}
Data export operations	2019-02-11 11:20:30,188 deviceVersion: "11.3.0.0" deviceService: "SA_SERVER" category: DATA_ACCESS operation: "submitExtractPcap" parameters: "deviceId=6 collectionName= predicateHandle=c6cf sessionIds=[9285468, 9286362, 9628535, 9629308, 10013047, 10017581, 10428756, 10439924, 10819088, 10820894, 11164416] startDate=2019-02-11T08:20:00.000Z endDate=2019-02-11T11:19:59.000Z id1=1 id2=287399592" outcome: "Success" identity: "admin" userRole: "Administrators"

The following table shows examples of Global Audit Logs using the default Common Event Format (CEF) template. 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.

User Actions	CEF Examples
User Login Success	May 23 2019 13:52:39 updatestackadminserver CEF:0|RSA|NetWitness Audit|11.3.1.0|Security|Logon-Web|6|rt=May 23 2019 13:52:39 scope=scope suser=AdminNorm sourceServiceName=admin-server deviceExternalId=eXXXX-4XXX-4XXX-8XXX-6dXXXXX09 deviceProcessName=ADMIN-SERVER outcome=success remoteAddress=110.10.10.1 uri=/oauth/token referrerURL=https://10.111.201.10/login
User Login Failure	May 23 2019 13:42:38 updatestackadminserver CEF:0|RSA|NetWitness Audit|11.3.1.0|Security|Logon-Web|6|rt=May 23 2019 13:42:38 scope=scope suser=AdminNorm sourceServiceName=admin-server deviceExternalId=eXXXX-4XXX-4XXX-8XXX-6XXXXXX09 deviceProcessName=ADMIN-SERVER outcome=failed remoteAddress=110.10.10.1 reasonForFailure=Bad credentials uri=/oauth/token referrerURL=https://10.111.201.10/login
User Logouts	Jun 06 2019 13:01:25 updatestackadminserver CEF:0|RSA|NetWitness Audit|11.3.1.0|Security|Logoff|6|rt=Jun 06 2019 13:01:25 scope=scope suser=admin sourceServiceName=admin-server deviceExternalId=e07b16f8-4xxx-4xx1-895b-6dxxxxx809 deviceProcessName=ADMIN-SERVER outcome=success remoteAddress=101.101.007.101 reason=User Triggered referrerURL=https://10.111.117.115/respond/incidents uri=/oauth/logout action=Logoff,"uri":"/oauth/logout”
All UI pages accessed	May 23 2019 14:01:13 updatestackadminserver CEF:0|RSA|NetWitness Audit|11.3.1.0|DATA_ACCESS|HttpRequest|6|rt=May 23 2019 14:01:13 scope=scope suser=AdminNorm userRole=Administrators sourceServiceName=SA_SERVER deviceExternalId=e0XXX8-4XXX-4XXX-8XXX-6XXXXXX09 deviceProcessName=SA_SERVER outcome=Success remoteAddress=110.11.10.1 uri=/admin/appliances referrerURL=https://10.111.201.10/admin/services May 23 2019 14:01:13 updatestackadminserver CEF:0|RSA|NetWitness Audit|11.3.1.0|SYSTEM|Page Accessed|6|rt=May 23 2019 14:01:13 scope=scope key=[ADM] Hosts suser=AdminNorm userRole=Administrators sourceServiceName=SA_SERVER deviceExternalId=e0XXXX-4XXX-4XXX-8XXX-6d5XXXXX09 deviceProcessName=SA_SERVER outcome=Success
Committed configuration changes	May 23 2019 14:08:03 updatestackadminserver CEF:0|RSA|NetWitness Audit|11.3.1.0|CONFIGURATION|Modified|6|rt=May 23 2019 14:08:03 scope=scope key=ntp-servers value={10.10.20.10\=true} suser=AdminNorm userRole=Administrators sourceServiceName=SA_SERVER deviceExternalId=e07XXX-4XXX1-4XXX-8XXX-6d5XXXXX809 deviceProcessName=SA_SERVER params=validate

User Actions	CEF Examples
Queries performed by the user	May 23 2019 14:12:32 updatestackadminserver CEF:0|RSA|NetWitness Audit|11.3.1.0|Predicate|update|6|rt=May 23 2019 14:12:32 scope=scope suser=AdminNorm sourceServiceName=investigate-server deviceExternalId=e0XXXX-4XXX-4XXX-8XXX-6d5XXXXX09 deviceProcessName=INVESTIGATE-SERVER outcome=success “updated":"UserPredicateEntity(id\=5cXXXXXXdd, userId\=AdminNorm, predicateEntity\=PredicateEntity (id\=ff53, legacyId\=null, query\=user.all\='solay', displayName\=user.all\='solay'), lastUsed\=2019-05-23T14:12:32.406Z)"}
Data export operations	May 23 2019 14:17:05 updatestackadminserver CEF:0|RSA|NetWitness Audit|11.3.1.0|DATA_ ACCESS|submitExtractPcap|6|rt=May 23 2019 14:17:05 scope=scope suser=AdminNorm userRole=Administrators sourceServiceName=SA_SERVER deviceExternalId=e0XXXX8-4XXX-4XXX-8XXX-6d5XXXXX9 deviceProcessName=SA_SERVER outcome=Success params=deviceId\=17 collectionName\= predicateHandle\=8629 sessionIds\=null startDate\=2019-05-23T10:59:00.000Z endDate\=2019-05-23T13:58:59.999Z id1\=1 id2\=393378

The following table shows examples of global audit logs using the default human-readable format template on a third-party syslog server.

User Actions	Human-Readable Format Output
User Login Success	Jun 11 2019 05:02:07 UpdateStackAdminServer Jun 11 2019 05:02:07 BROKER [audit] Event Category: AUTHENTICATION Operation: login Outcome: success Description: null User: admin Role: admin.owner, aggregate,concentrator.manage,connections.manage,everyone,index. manage,logs.manage,sdk.content,sdk.manage,sdk.meta,sdk.packets, services.manage,storedproc.execute,storedproc.manage,sys.manage, users.manage params=null
User Login Failure	Jun 11 2019 05:22:11 updatestackadminserver Jun 11 2019 05:22:11 admin-server [audit] Event Category: Security Operation: Logon-Web Outcome: failed Description: null User: admin Role: null params= {"referrer":"https://10.101.101.101/login","method":"POST", "reasonForFailure":"Bad credentials","userAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.80 Safari/537.36","uri":"/oauth/token", "remoteAddress": "10.101.102.103"}

User Actions	Human-Readable Format Output
User Logouts	Jun 11 2019 02:06:24 updatestackadminserver Jun 11 2019 02:06:24 admin-server [audit] Event Category: Security Operation: Logoff Outcome: success Description: null User: admin Role: null params ={"reason":"User Triggered","referrer":"https://10.101.101.101/respond/incidents","method":"POST","userAgent":"Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36","uri":"/oauth/logout", "remoteAddress":"10.101.102.103"}
All UI pages accessed	Jun 11 2019 02:06:25 updatestackadminserver Jun 11 2019 02:06:25 SA_SERVER [audit] Event Category: DATA_ACCESS Operation: Http Request Outcome: Success Description: null User: Unknown identityRole: null params= {referrer\=https://10.101.101.101/login, method\=GET, X-Forwarded-For\=10.201.111.111, userAgent\=Mozilla/ 5.0 (Windows NT 10.0; WOW64)AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36,queryString\=, uri\=/display/ security/securitybanner/get, remoteAddress\=10.101.102.103}
Committed configuration changes	Jun 11 2019 02:08:13 updatestackadminserver Jun 11 2019 02:08:13 security-server [audit] Event Category: Authorization Operation: update Outcome: success Description: null User: admin Role: null params={"Role":"analystl1","Add.Permission":"[admin-server.process.manage, admin-server.configuration.manage, admin-server. health.read, admin-server.security.manage, admin-server.metrics. read, admin-server.security.read, admin-server.logs.manage]"}

User Actions	Human-Readable Format Output
Queries performed by the user	Jun 11 2019 02:12:57 UpdateStackConcentrator Jun 11 2019 02:12:57 CONCENTRATOR[audit] Event Category: DATA_ACCESS Operation: query Outcome: success Description:has finished query (channel 2085, queued 00:00:00, execute 00:00:00) User: adminRole: null params= queryPriority\=20 id1\=1 id2\=324751797 size\=0 flags\=0 threshold\=0 query\="select event.time , sessionid , alias.host, reference.id ,host.src , user.dst , event.type , result.code , event.source.id , host.dst ,service.name , logon.type , device .type , event.cat.name , ec.activity , ec.outcome,analysis. service , event.desc , action , user.src , result where ((reference.id \='4624','4625','4769','4648') || (device.type \= 'rsaacesrv' && ec.activity \= 'Logon') || ((action \= '/usr/sbin/sshd' || action\='/usr/bin/login') && device.type \= 'rhlinux')) and event.time \= 1539444840-1539444899 "
Data export operations	Jun 11 2019 02:14:04 updatestackadminserver Jun 11 2019 02:14:04 SA_SERVER [audit] Event Category: DATA_ACCESS Operation: submit ExtractLogs Outcome: Success Description: null User: admin Role: Administrators params=deviceId\=17 collectionName\=predicate Handle\= sessionIds\=null exportFormat\=RAWLOGS startDate\=2019- 06-10T23:14:00.000Z endDate\=2019-06-11T02:13:59.999Z id1\=1 id2\ =1694664

For lists of message type being logged by the various NetWitness components, see Global Audit Logging Operation Reference.

Supported CEF Meta Keys

This topic describes the Common Event Format (CEF) meta keys that NetWitness 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 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
Syslog Prefix				
Datetime	Not Configurable	Syslog Header date time	event.time.str	Transient
Hostname	Not Configurable	Syslog Header hostname	alias.host	None
CEF Header		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, NetWitness	-	N/A
DeviceProduct	%{deviceProduct}	The product family. This is always NetWitness Audit.	product	Transient
DeviceVersion	%{deviceVersion}	Host/Service version	version	Transient

CEF Field	String	Description	NW Meta Keys	Index in Log Decoder
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
Extensions				
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	%{destinationAddress}	Destination IP Address	ip.dst	None
dvcpid	%{deviceProcessId}	ID of the process generating the event, which is the process ID of the NetWitness service	process.id	Transient
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
tpt	%{transportProtocol}	Network protocol used	protocol	Transient
userAgent	%{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	%{deviceService}	The service that is responsible for generating this event	service.name	Transient

CEF Field	String	Description	NW Meta Keys	Index in Log Decoder
spt	%{sourcePort}	Source Port	ip.srcport	Transient
userRole	%{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	user.role	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
Custom Extensions				
params	%{parameters}	API and Operation parameters, which capture specific parameters about a query	index	Transient
paramKey	%{key}	A configuration item key. It is the config param for which the audit event is captured. For example: /sys/config/stat.interval	obj.name	None
paramValue	%{value}	A configuration value. It is the value captured during the update.	no meta key	Custom
userGroup	%{userGroup}	Role assignment. For example: Administrators, Analysts, MalwareAnalysts, Malware_Analysts, Operators, PRIVILEGED_CONNECTION_AUTHORITY, SOC_Managers	group	None

CEF Field	String	Description	NW Meta Keys	Index in Log Decoder
referrerURL	%{referrer}	The parent URL that refers to the current URL	referer	None
sessionId	%{sessionId}	Session or connection identifier	log.session.id	Transient
remoteAddress	%{remoteAddress}	Ip address of the destination	ip.src	None
reasonForFailure	%{reasonForFailure}	reason for failure for the certain action performed	result	None
reason	%{reason}	Reason for certain action performed	result	None
addRole	%{Add.Role}	User role Assignment	user.role	Transient
id	%{id}	Incident id or host id	no meta key	Transient
arguments	%{arguments}	Value passes between programs or functions	index	Transient
uri	%{uri}	Directory	directory	None
user	%{User}	Name of the user from the source or destination	user.dst	None
accountProvider	%{AccountProvider}	Authentication account for the user. For example, PAM, and PKI.	index	Transient
file	%{file}	Name of the content file used for deployment	filename	File
deviceIDs	%{deviceIDs}	Device id for the particular service	hardware.id	Transient
role	%{Role}	User role assignment	user.role	Transient
account	%{Account}	user account	user.dst	None
addPermission	%{Add.Permission}	User role permission assignment	permissions	Transient
key	%{Key}	Name of a configuration/rule	obj.name	None
value	%{Value}	Value of a configuration change. For example, "Value":"HR12". In this example, hours format is changed to 12 hours.	no meta key	Custom

CEF Field	String	Description	NW Meta Keys	Index in Log Decoder
alert	%(alert}	Id of the alert, For example, id:5ce457afec6c0f02ffb85ace	alert	Transient
moduleSettings	%{ModuleSettings}	Message or name of a setting	index	Transient
incident	%{incident}	Id of the incident. For example, INC-313	context	None
action	%{action}	Action performed by the user. For example, service.stop	action	None
notificationBinding	%{NotificationBinding}	Type of notification. For example, incident created, alert, incident removed	index	Transient
name	%{name}	name of a configuration or rule	alert	Transient
enabled	%{enabled}	Enable the rule	no meta key	Custom
disabled	%{disabled}	Disable the rule	no meta key	Custom

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.

For more information, see the following documentation:

- The "Maintain the Table Map Files" section in the "Hosts and Services Procedures" topic in the *Hosts and Services Getting Started Guide* provides instructions for verifying and updating the table mappings.
- The "Edit a Service Index File" section in the "Hosts and Services Procedures" topic in the *Hosts and Services Getting Started Guide* 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 global audit logging supports.

NetWitness 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 global audit logging supports. Use these values to create a custom audit logging template for a third-party syslog server.

Variable	Description
%{category}	Identifier of the audit event. It specifies the the category of the audit event.
%{destinationAddress}	Destination IP Address
%{destinationPort}	Destination Port
%{deviceExternalId}	Unique ID of the service generating the audit event
%{deviceFacility}	Syslog facility used when writing the event to syslog daemon. For example, authpriv.
%{deviceProcessId}	ID of the process generating the event, which is the process ID of the NetWitness service
%{deviceProcessName}	Name of the executable corresponding to dvcpid
%{deviceProduct}	The product family. This is always NetWitness Audit.
%{deviceService}	Service responsible for generating the event
%{deviceVendor}	The product vendor, RSA
%{deviceVersion}	Host/Service version
%{identity}	Identity of the logged on user responsible for generating the audit event
%{key}	A configuration item key. It is the config param for which the audit event is captured.
%{operation}	Description of the event

Variable	Description
%{outcome}	Outcome of the operation performed corresponding to the audit event
%{parameters}	API and Operation parameters, which capture specific parameters about a query
%{referrerUrl}	The parent URL that refers to the current URL
%{sessionId}	Session or connection identifier
%{severity}	Severity of the audit event
%{sourceAddress}	Source IP Address
%{sourcePort}	Source Port
%{sourceService}	The service that is responsible for generating this event
%{text}	Free text, extra information, or actual description for the event
%{timestamp}	Time at which the event is reported
%{transportProtocol}	Network protocol used
%{userAgent}	Browser detail of the user accessing the page
%{userGroup}	Role assignment
%{userRole}	User role permissions assignment
%{value}	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 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 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 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

Serial #	Operation Name	Meaning
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.
12	userPredicates	Operation to access Recent Queries of a user.

Serial #	Operation Name	Meaning
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 asTime 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.
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.
36	SaveProfile	Operation to save an Investigation Profile.
37	ApplyProfile	Operation to apply an Investigation Profile.

Serial #	Operation Name	Meaning
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
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

Serial #	Operation Name	Meaning
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.
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 Core Services

The following table lists the operations logged by NetWitness 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
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.

Serial #	Operation Name	Meaning
25	reload	Issuing a parser reload
26	schema	Issuing a schema request for loaded parsers
27	upload/file.upload	Issuing file upload
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
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

Serial #	Operation Name	Meaning
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
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
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

Serial #	Operation Name	Meaning
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
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	CountByMetaNameAndValueWithDate RangeIntervalRequest	Count meta and values with interval for charting
20	CountByValueAndAverageOverallScore Request	Count meta and map to overall scores for events
21	CountByValueAndAverageGroupScore Request	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

Serial #	Operation Name	Meaning
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
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
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

Serial #	Operation Name	Meaning
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
66	Logon	Logon to the MA Service
67	Modified	Modifying config changes
68	GetNextGenSummaryRequest	Get nextgen dashboard summary statistics

NetWitness User Interface

The following table lists the operations logged by the NetWitness 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

Serial #	Operation Name	Meaning
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
14	uploadOfflineResponse	Upload offline response
15	offlineDownloadCapRequest	Download offline request
16	movePerpetualToThroughput	Move Appliance license to Throughput
17	moveThroughputToPerpetual	Mover Throughput to Appliance license
18	mapApplianceLicense	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.
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.

Serial #	Operation Name	Meaning
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.
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.

Serial #	Operation Name	Meaning
48	deleteEndpointCache	Operation to clear reconstruction cache of a device.
49	Logon	Operation for user to sign in to NetWitness User Interface.
50	Logoff	Operation for user to sign out of NetWitness 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.
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.

Serial #	Operation Name	Meaning
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
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

Investigate Server

Serial #	Operation name	Meaning
1	Aliases	Fetch aliases
2	BackgroundJob	Category for all background job
3	ColumnGroup	Category for all column group operation

Serial #	Operation name	Meaning
4	Count-query	Default Investigate
5	Countdistict-query	Default Investigate
6	Content	Default Session Content
7	Create	User entity
8	Create	User preferences
9	Create	Predicate
10	Delete	User preferences
11	Delete	Predicate
12	Extract-content	Extract Content from Session
13	Folders	Category for all folder operation
14	Files	SDK content request
15	InvestigateExport	Category for extraction invocation
16	Key-refs	Fetch meta keys
17	Languages	SDK language call
18	MetaGroup	Category for all meta group operation
19	Metakey	Category for all metakey operation
20	MailReconstruction	Category for all mail reconstruction operation
21	ParsingRequest	Category for all request parsing operation
22	PacketReconstruction	Category for all packet reconstruction operation
23	Predicate InvestigateIncidents	Category for all predicate operation
24	Query	SDK query
25	Reconstruction	Category for common shared reconstruction operation
26	ReconstructionCache	Category for reconstruction caching operation
27	ReconstructionStreaming	Category for reconstruction streaming operation
28	ReconstructDataSecurity	Category for reconstruction security operations (data-scrubbing)
29	Session-Meta	SDK query to get session meta

Serial #	Operation name	Meaning
30	Summary	SDK summary
31	Search-meta-value	Search meta-value based on field name
32	TextReconstruction	Category for all text reconstruction operation
33	Timeline	Timeline request
34	UserPreferences	Category for all user preferences operation
35	Update	User entity
36	Update	User preferences
37	Update	Profile group
38	Update	Predicate
39	Values	SDK values
40	Validate-query	Validate SDK query

Security Server

The following table lists the events logged by the Security Server.

Log Category	Description
Create:	Add record for a role with new ID.
Create:	Add user record with new ID.
Update:	Update the user account with a new ID.
Authentication:	Logs events pertaining to user logins and logouts.
Authorization:	Logs events pertaining to user access checks and RBAC management.
UserAccount	Logs events pertaining to NetWitness domain account management.
ExternalProvider:	Tracks events pertaining with external account providers (for example, Active Directory).

The following example shows an event logged by the Security Server:

```
2018-03-13 16:25:02,938 UserAccount{action=ExpirePassword, success=true,
identity=admin, parameters={id=Justin}}
```

Admin Server

The following table lists the events logged by the Admin Server.

Log Category	Description
Restore:	System operation to restore a data springboard.

Config Server

The following table lists the events logged by the Admin Server.

Log Category	Description
newregistration:	Record the registration to config server that manages the collection storage.

Context Hub Server

The following table lists the events logged by the Admin Server.

Log Category	Description
verifyconnection:	System operation to check if the connection is live.
addconnection	Create new connection to access data.

Local Audit Log Locations

NetWitness has global audit logging capabilities. When you configure global audit logging, audit logs from all NetWitness 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 user interface and the various NetWitness services.

Service/Module	Audit Log Location
NetWitness User Interface (NetWitness Web Server)	The NetWitness user interface sends audit logs to the following locations: • `/var/lib/netwitness/uax/logs/audit/audit.log` (human-readable format) • Syslog running on the local host (JSON format) The NetWitness user interface uses the AUTH facility of syslog to write audit logs to syslog. You can only see audit logs in the first location (`/var/lib/netwitness/uax/logs/audit/audit.log`).
Core Services (Decoder, Log Decoder, Concentrator, Broker, and Archiver), Log Collector, Warehouse Connector, and Workbench	The Core services and similar services send audit logs to Syslog running on the local host. Path: `/var/log/secure` (JSON format) The Core services use the AUTHPRIV facility of syslog to write audit logs to syslog.

Service/Module	Audit Log Location

Reporting Engine,
Malware Analysis,
Respond,
ESA Correlation (11.3 and later),
and Event Stream Analysis
(11.2 and earlier)
	These services send audit logs to the following locations:
	• `<application-home-directory>/logs/audit/audit.log` (human-readable format)
	• Syslog running on the local host (JSON format)
	
	The following are the audit log locations of these services:
	Reporting Engine:
	`/var/netwitness/re-server/rsa/soc/reporting-engine/logs/audit/audit.log`
	Respond Server:
	`/var/log/netwitness/respond-server/respond-server.audit.log`
	Malware Analysis:
	`/var/lib/netwitness/malware-analytics-server/spectrum/logs/audit/audit.log`
	ESA Correlation (11.3 and later):
	`/var/log/netwitness/correlation-server/correlation-server.audit.log`
	Event Stream Analysis (11.2 and earlier):
	`/opt/rsa/esa/logs/audit/audit.log`
	These services use the AUTH facility of syslog to write audit logs to syslog. You can only see audit logs in the first location (`<application-home-directory>/logs/audit/audit.log`).

Health & Wellness, Event Source Management (ESM), and Appliance and Service Grouping (ASG)	These Services send audit logs to the following locations: • `/opt/rsa/sms/logs/audit/audit.log` (human-readable format) • Syslog running on the local host (JSON format) 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`).
Aggregated Audit Logs	The aggregated audit logs from all the services are sent to the following locations: • `/var/netwitness/logstash/logs/rsa-netwitness-audit.log` (JSON format) • Syslog running on the local host (human-readable format)

Global Notifications Panel

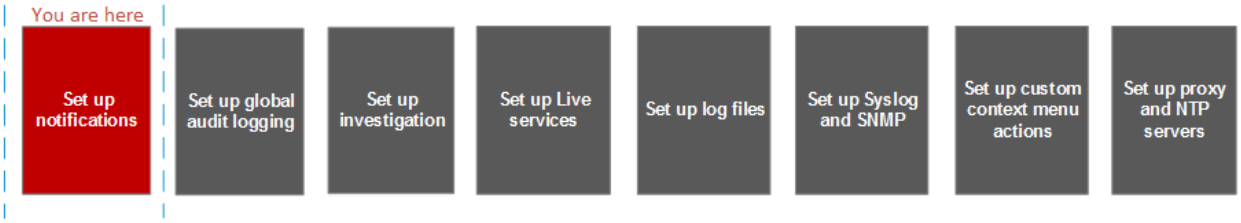
Global Notifications panel introduces the features for configuring notification settings. Global Notifications configurations define notifications settings for Event Source Management (ESM), Health and Wellness, Global Audit Logging, Event Stream Analysis (ESA), and Respond.

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

- Notification Outputs
- Notification Servers
- Templates

Note: ESA SNMP notifications are not supported for NetWitness 11.3 and later.

WorkFlow



What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure Notification Servers	Servers Tab
Administrator	Configure Notification Outputs	Output Tab
Administrator	Configure Notification Templates	Templates Tab

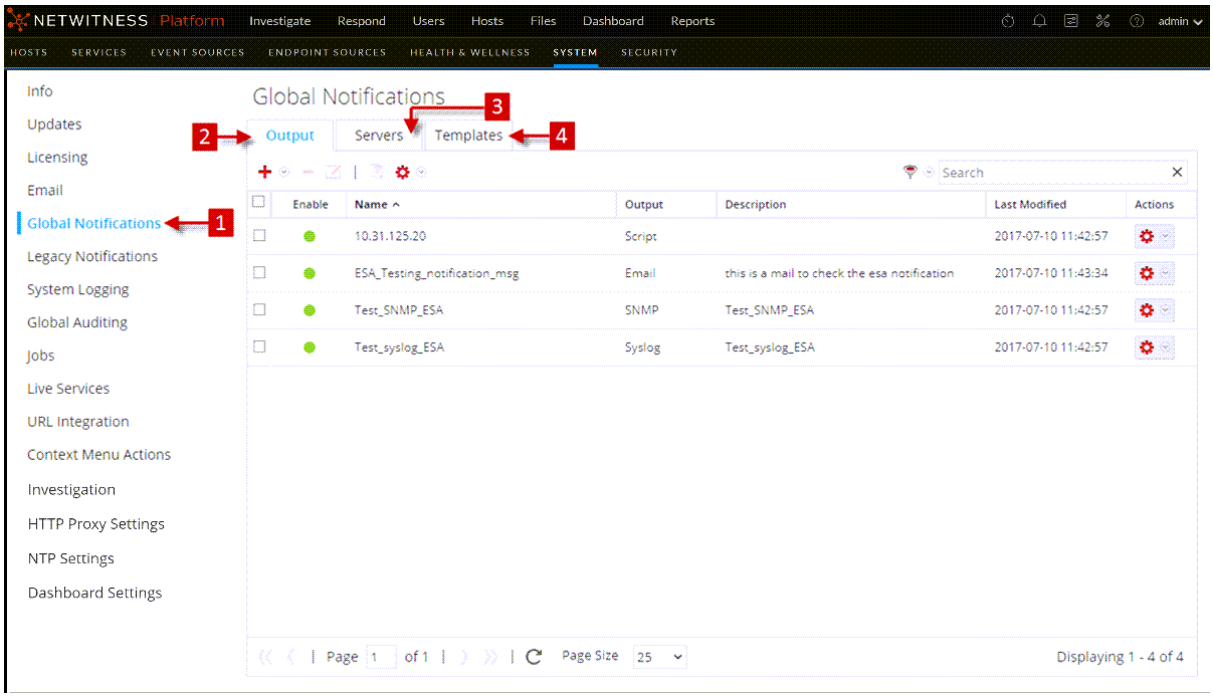
Related Topics

- Configure a Syslog Notification Server
- Configure Script as a Notification Server

Quick Look

To access the Notifications configuration panel:

1. In the main menu, select (Admin) > **System**.
2. In the options panel, select **Global Notifications.**



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
Output tab	This tab enables you to configure notification outputs. See Output Tab for more information.
Servers tab	This tab enables you to configure notification servers. See Servers Tab for more information.
Templates tab	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.
Enable	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.
Name	A name that identifies or labels the configuration.
Output	The configuration output. The outputs are Email, SNMP, Syslog, and Script.
Description	A brief description about the configuration.
Last Modified	Shows the date and time of the last configuration change.
Actions	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.

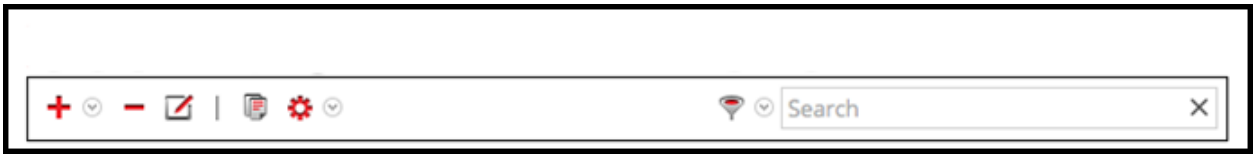
This table describes the columns in the grid for Notification Templates.

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.
Name	A name that identifies or labels the template.
Template Type	The type of template. The types are Audit Logging, Event Stream Analysis, Event Source Monitoring, and Health Alarms.
Description	A brief description about the template.
Actions	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

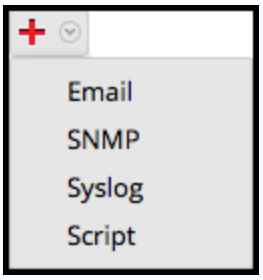
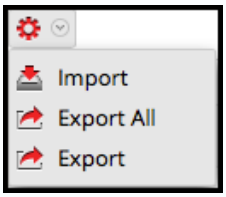
The Global Notifications panel toolbar is at the top of the Output, Servers, and Templates tabs.

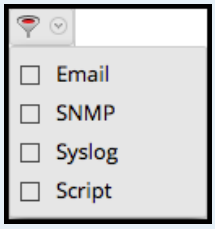
The following figure shows the toolbar on the Output and Servers tabs.



The following figure shows the toolbar on the Templates tab.

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

Feature	Description
 	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. On the Servers and Output tabs, you can select to configure Email, SNMP, Syslog, and Script notification settings.
	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.
	Edits a selected notification configuration. You can also edit a configuration by selecting a configuration and then in the Actions column, selecting  > Edit.
	Duplicates a selected notification configuration. You can also duplicate a configuration by selecting a configuration and then in the Actions column, selecting  > Duplicate.
	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.

Feature	Description
	Filters by Email, SNMP, Syslog, or Script.
	Searches configurations in the grid.

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 (Admin) > **System** > **Global Notifications** > **Servers** tab.

Notifications are used by a variety of components in NetWitness, 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:

- 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

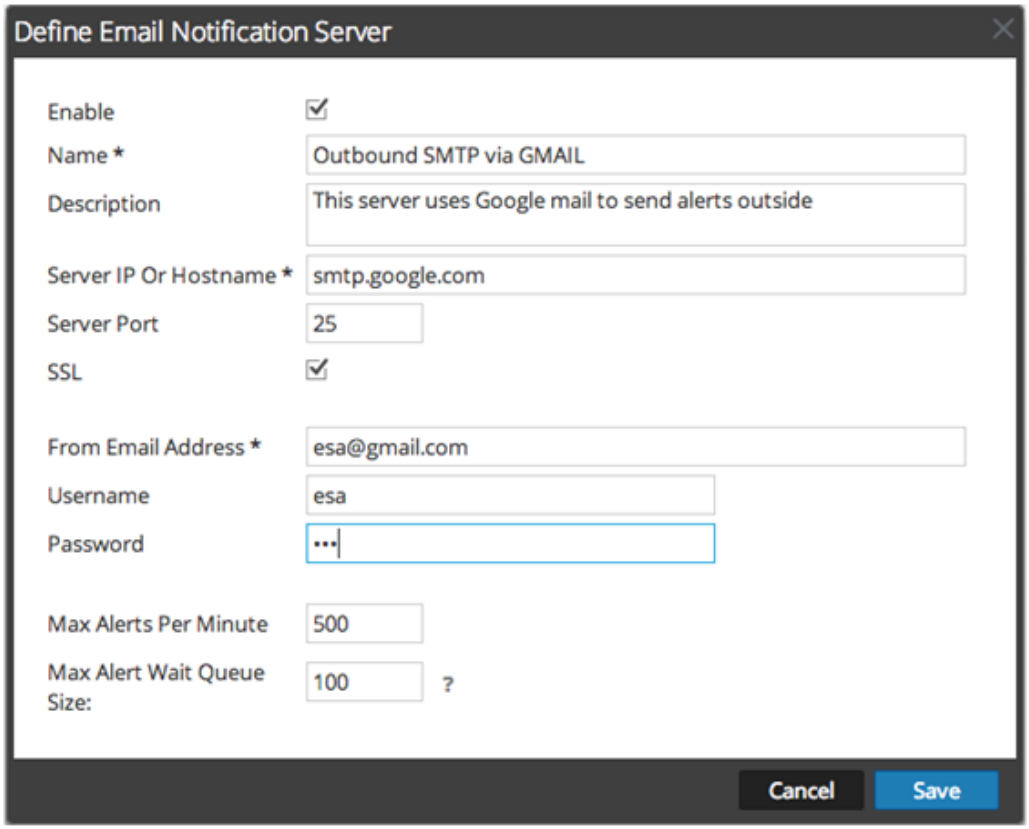
1. Go to **(Admin) > System**.
2. In the left navigation panel, select **Global Notifications**.
3. In the **Notifications Servers** panel, click and then select a type of notification server (Email, SNMP, Syslog, or Script)
   The Define Notification Server dialog is displayed for your selection.

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

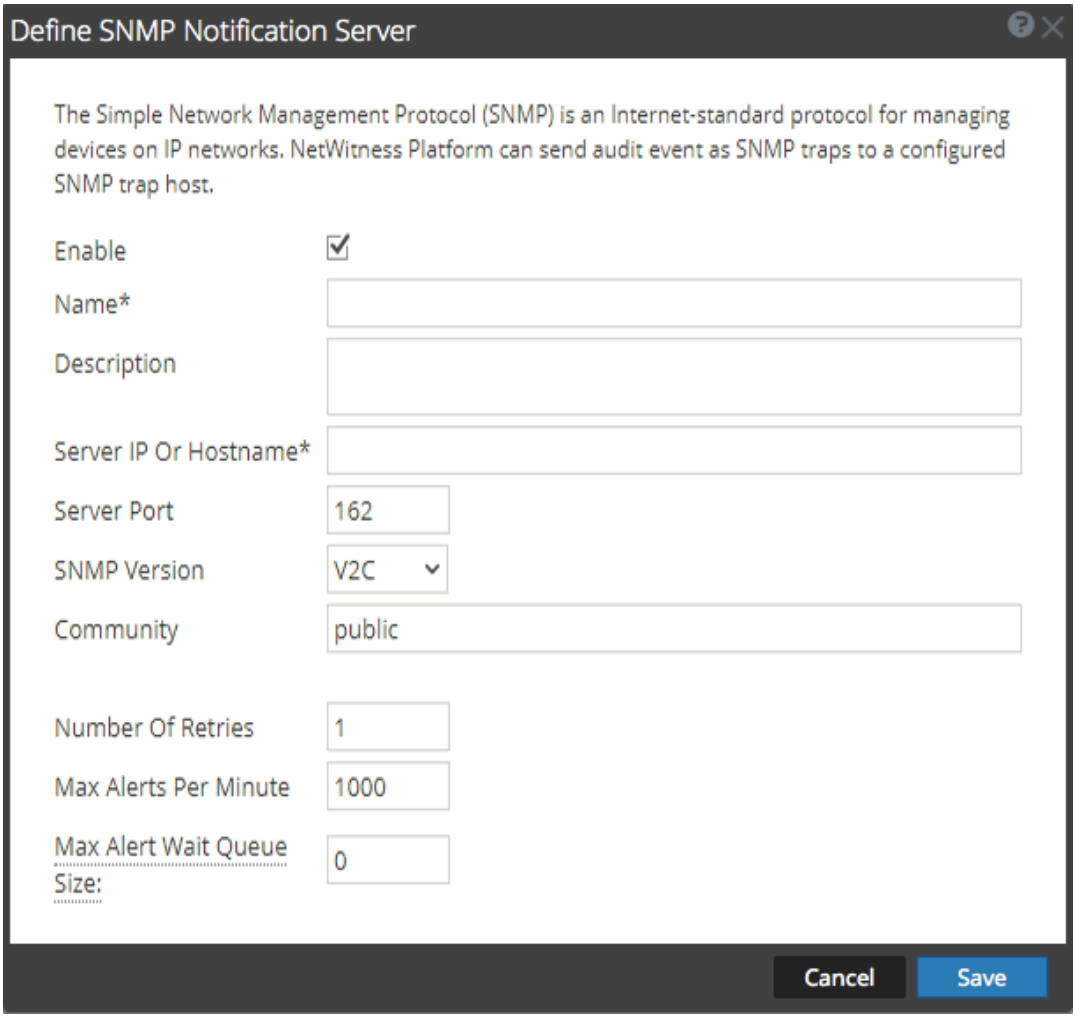
Parameters	Description
Enable	Select to enable the notification server.
Name	A name to identify or label the notification server.
Description	A brief description about the notification server.
Server IP Or Hostname	Hostname of the email server. For ESM/SMS and ESA notifications, you must specify only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

Parameters	Description
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.



The following table lists the various parameters that you need to define for the SNMP 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	SNMP trap host IP address or hostname.
Server Port	Listening port number on the SNMP trap host.

<table>
<tr><th>Parameters</th><th>Description</th></tr>
<tr><td>SNMP Version</td><td>SNMP version. The following are the options:
V1
V2C
V3
If you select SNMP Version 3 (v3), the following parameters are displayed:
<table>
<tr><th>Parameters</th><th>Description</th></tr>
<tr><td>Notification Type</td><td>Based on the notification type a SNMP messages are sent each time an alert is generated.
The following notification types are supported:
Inform - Inform is acknowledged trap. The sender gets an acknowledgement from the receiver.
Trap - Trap is unacknowledged notification</td></tr>
<tr><td>Authoritative Engine ID (This optioin is availabe only for notification type TRAP)</td><td>An identifier which is used to identify the agents. Authoritative engine ID along with the username is used to uniquely identify the agent.</td></tr>
<tr><td>Security Level</td><td>Define the security level. The following are the options:
Unauthenticated and Unencrypted
Authenticated and Unencrypted
Authenticated and Encrypted</td></tr>
<tr><td>Auth Protocol (This option is available only for security level Authenticated and Unencrypted and Authenticated and Encrypted)</td><td>Authentication protocol which is used to validate a user before providing an access to the server. The options are:
SHA
MD5</td></tr>
<tr><td>Auth Key (This option is available only for security level Authenticated and</td><td>A password that you want to use for authentication.</td></tr>
</table></td></tr>
</table>

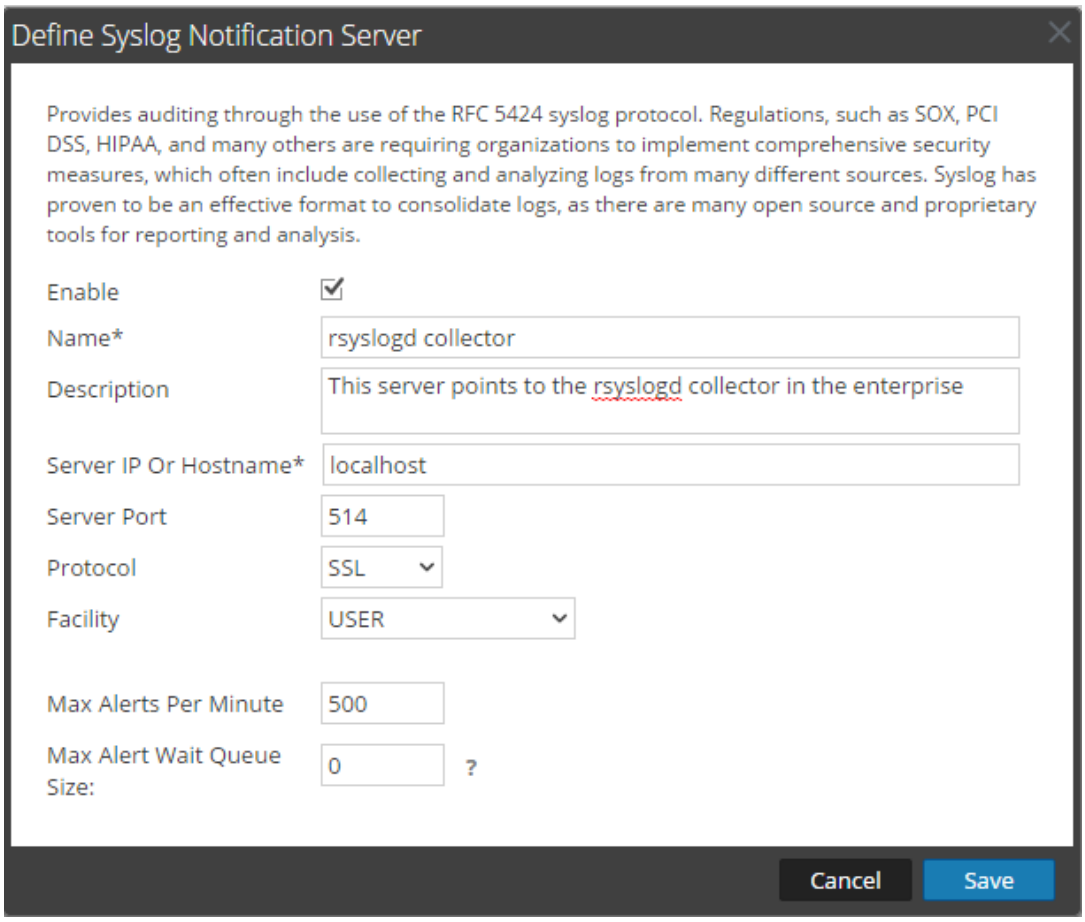
Parameters	Description
	Unencrypted and Authenticated and Encrypted) Privacy Protocol (This option is available only for security level Authenticated and Encrypted) — Privacy protocol is an encryption technique for data communication. Private Key (This option is avaliable only for security level Authenticated 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 **public**.
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.



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

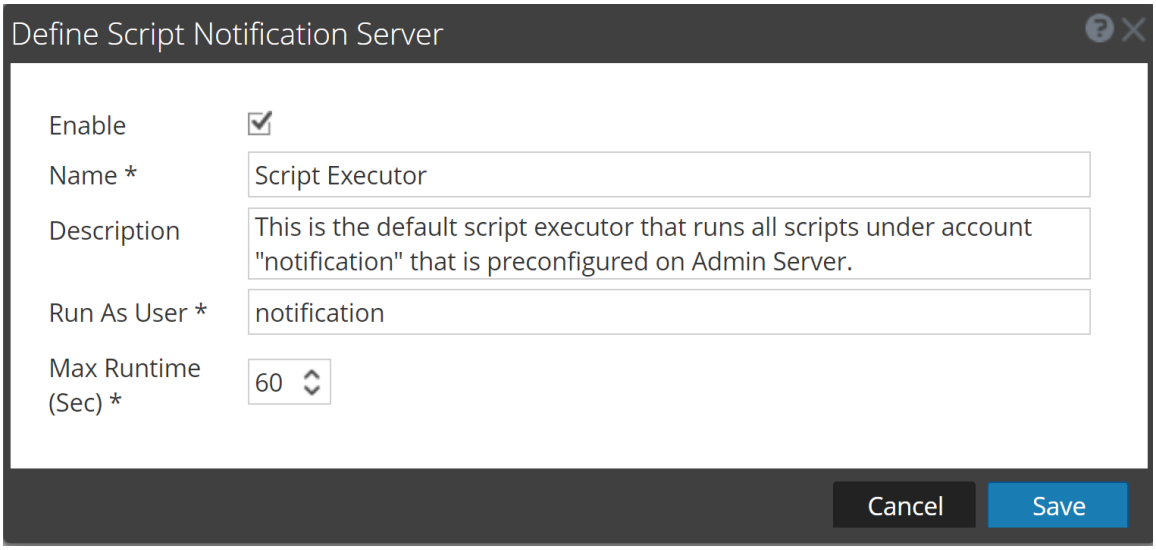
Parameters	Description
Enable	Select to enable the notification server.
Name	A name to identify or label the notification server.
Description	A brief description about the notification server.
Server IP Or Hostname	The hostname of the host where the target Syslog process is running.
Server Port	The port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

Parameters	Description
Max Alerts Per Minute	Maximum number of alerts per minute. This field is not used for Global Audit Logging.
Max Alert Wait Queue Size	Maximum number of alerts to be queued before they are dropped. This field is not used for Global Audit Logging.

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.
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 **notification**. For ESA, you cannot set this to anything else unless you have created the account on the Admin Server.
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 > Global 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:

- 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.

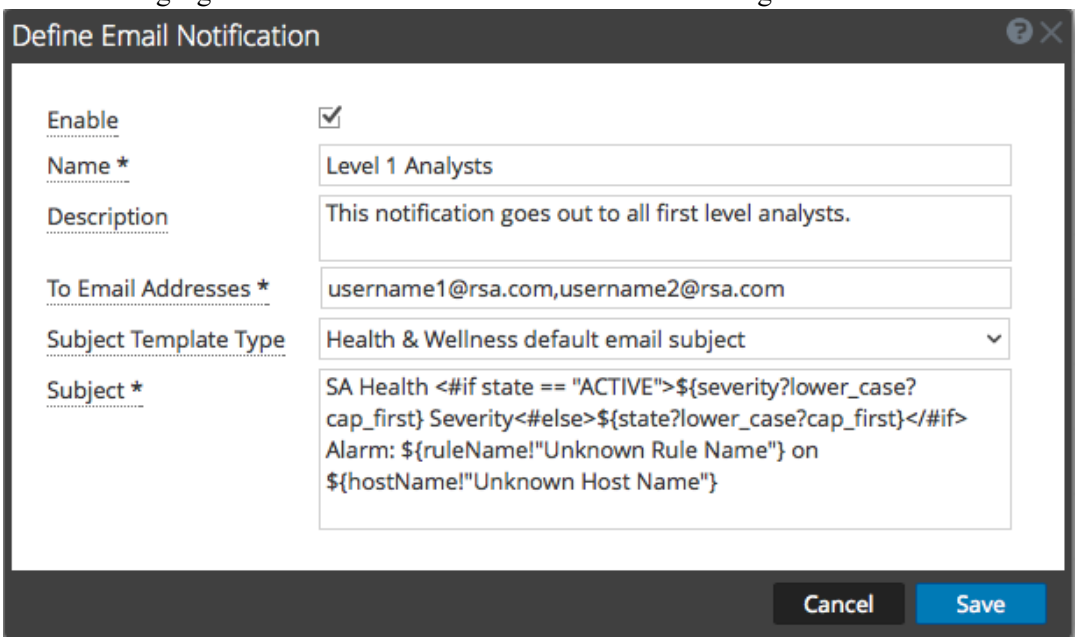
Features

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.



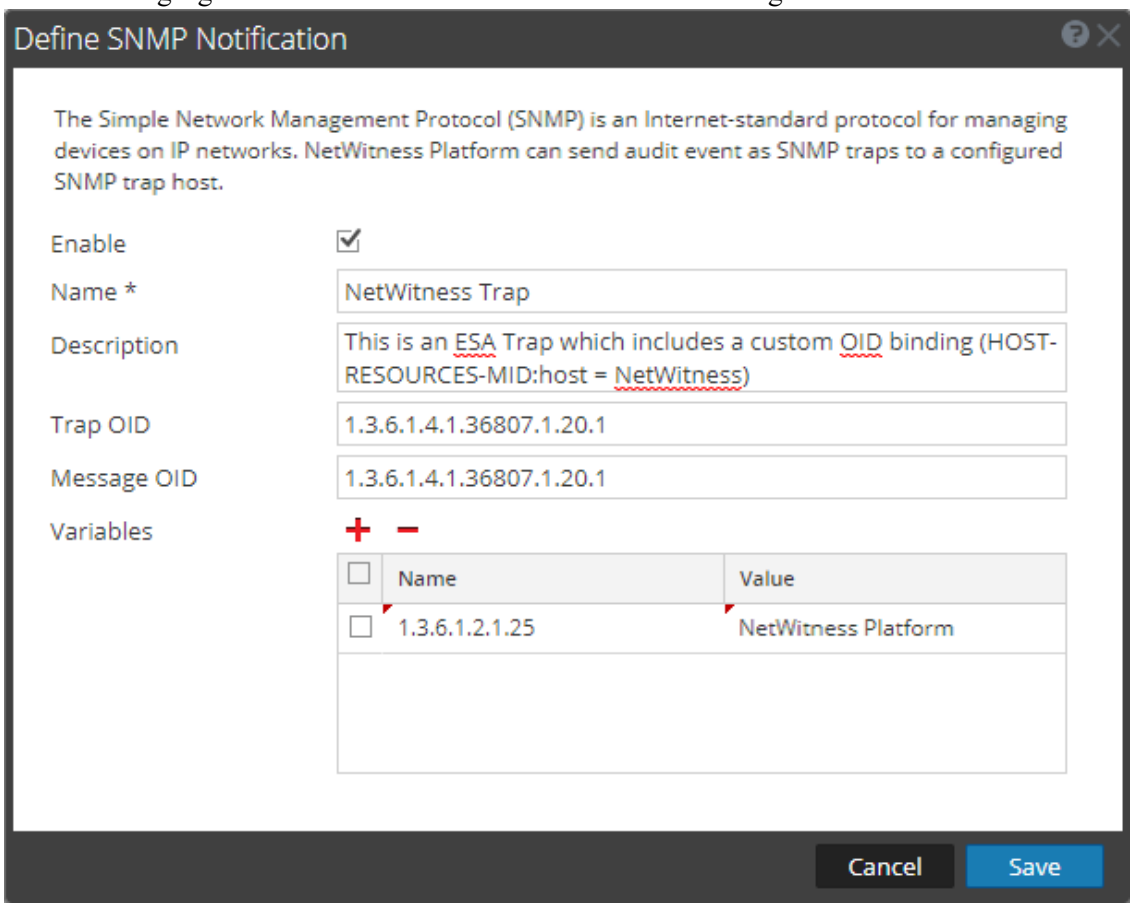
The following table lists the various parameters that you need to define for the email notifications.

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. **Note:** 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. Example, for New Health and Wellness, you must select **New Health & Wellness default email subject**.
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. **Note:** To provide a custom subject, please refer to "Include the Default Email Subject Line" topic in the *System Maintenance Guide*.

SNMP

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

The following figure shows the Define SNMP Notification dialog.



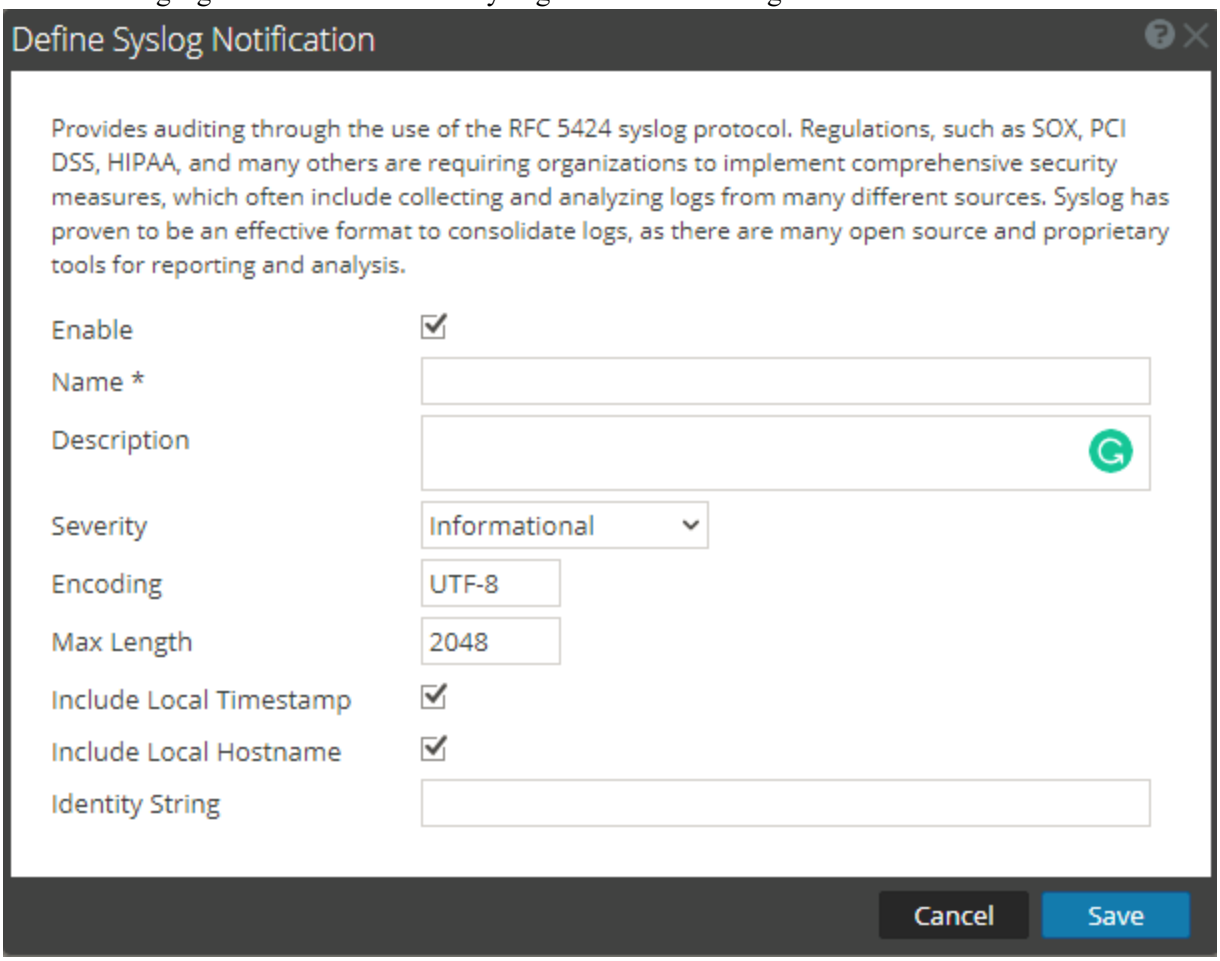
The following table lists the various parameters that you need to define for the SNMP notifications.

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 **1.3.6.1.4.1.36807.1.20.1**. 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.
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.



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

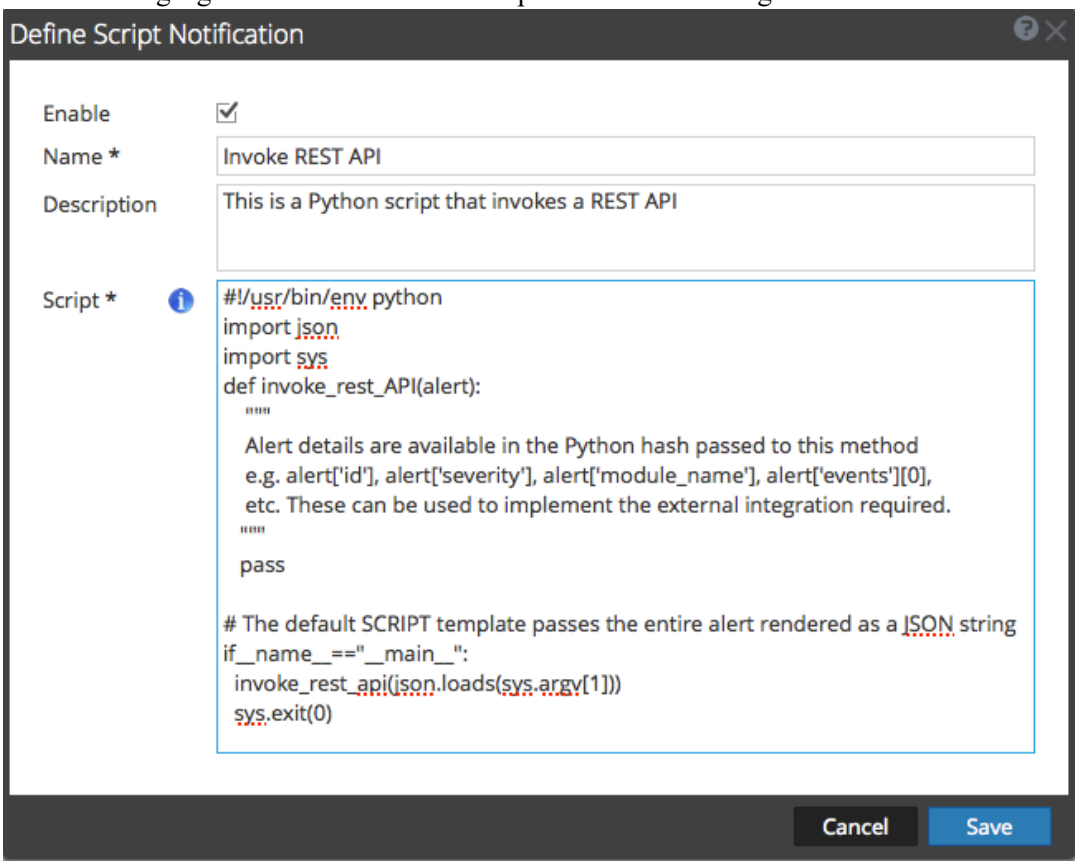
Parameter	Description
Enable	Select to enable the notification.
Name	A name to identify or label the notification.
Description	A brief description about the notification.
Severity	Defines the severity of the alert.
Encoding	Defines the encoding format. In some environments where no regular character 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 **2048**. Messages that exceed the maximum length are truncated when the **Truncate overly large syslog messages** checkbox is selected, which is found in Administration > System > Legacy Notifications. Legacy Notifications Configuration Panel provides additional information.

Parameter	Description
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.



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.

Parameter	Description
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 select a default template and use it or modify a default template based on your requirement. You can also use one of the following template types and create a template:

- Audit Logging
- Event Stream Analysis
- Event Source Monitoring
- Health Alarms
- New Health & Wellness Alarms.

These notification templates are created in an HTML, FreeMarker (FTL) format, a combination of both HTML and FTL, or Common Event Format (CEF) format:

- Email (SMTP) notification output type is created in both HTML and FTL formats.
- SNMP and Script notification output types are created in FTL format.
- Syslog notification output type is created in CEF format.

You need to have a good understanding of HTML, FTL, and CEF formats to successfully configure your own notification template. Click on the respective links to understand the specific formats.

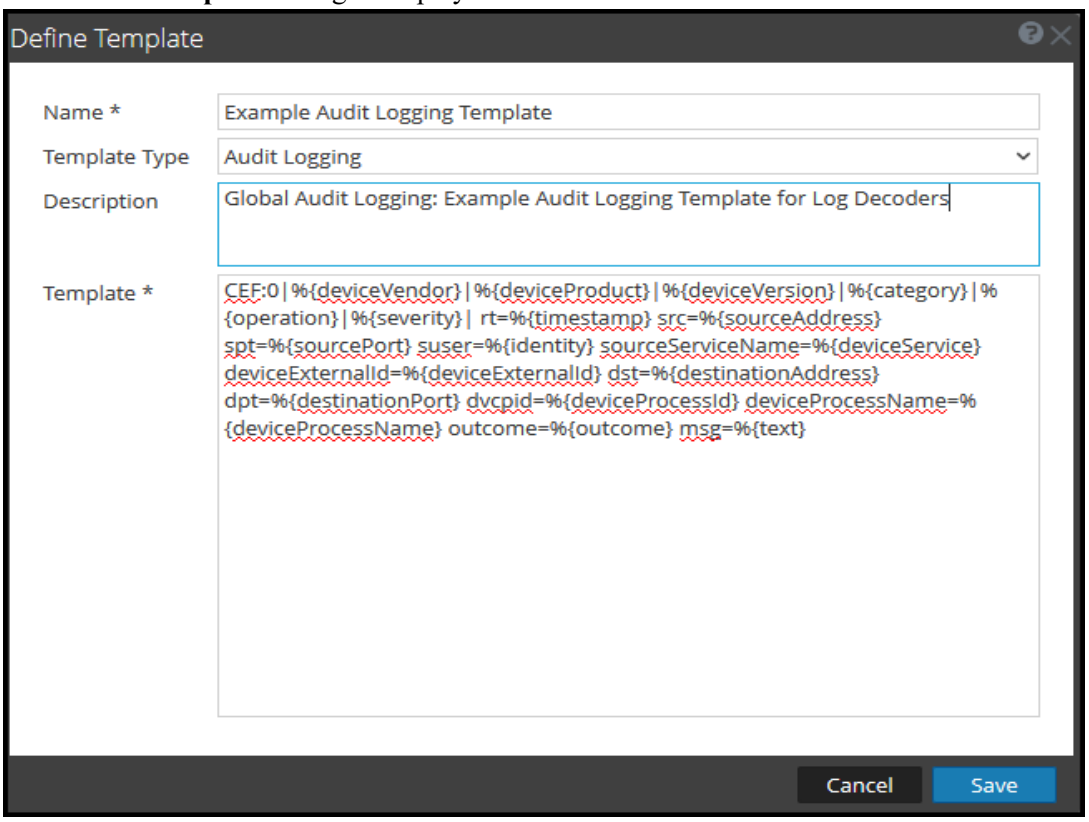
- HTML format, Introduction to HTML.
- FTL format, Overall structure - Apache FreeMarker Manual.
- CEF format, Freemarker Tips & Tricks in NetWitness.

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  to modify.

The **Define Template** dialog is displayed.

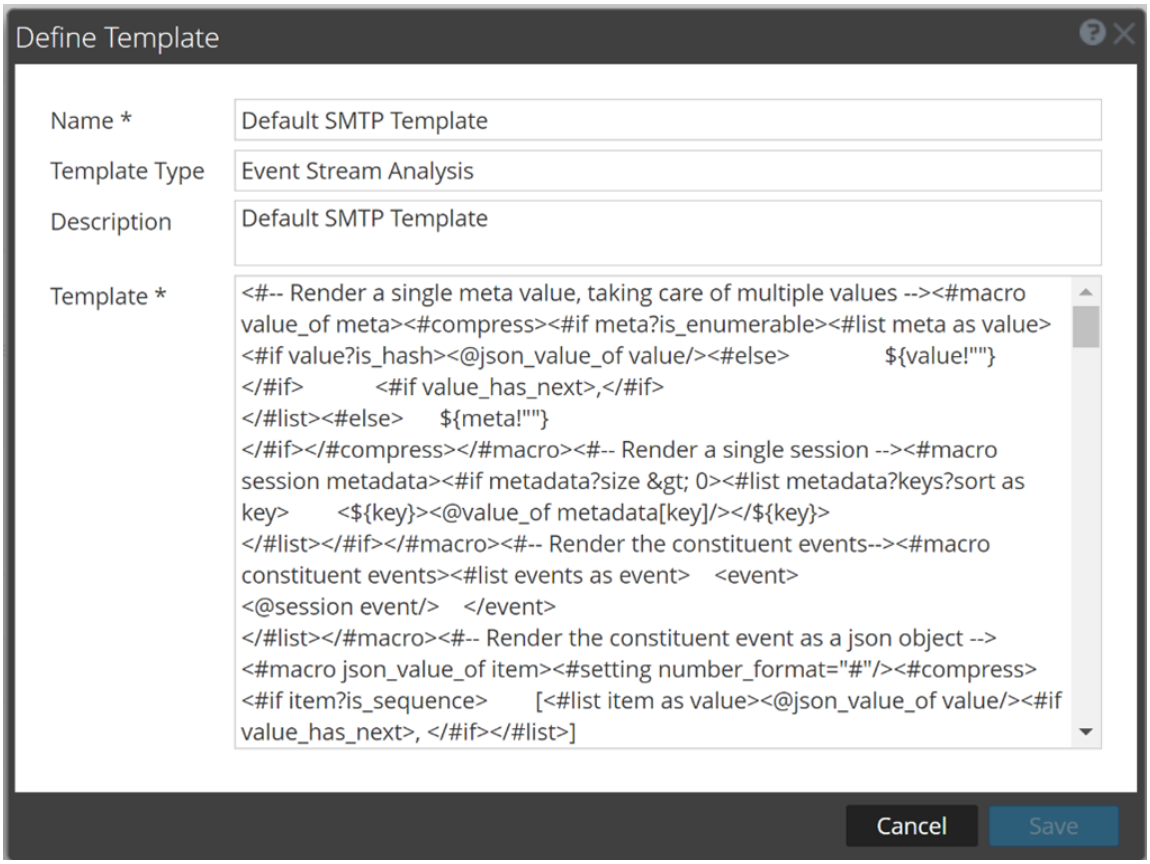


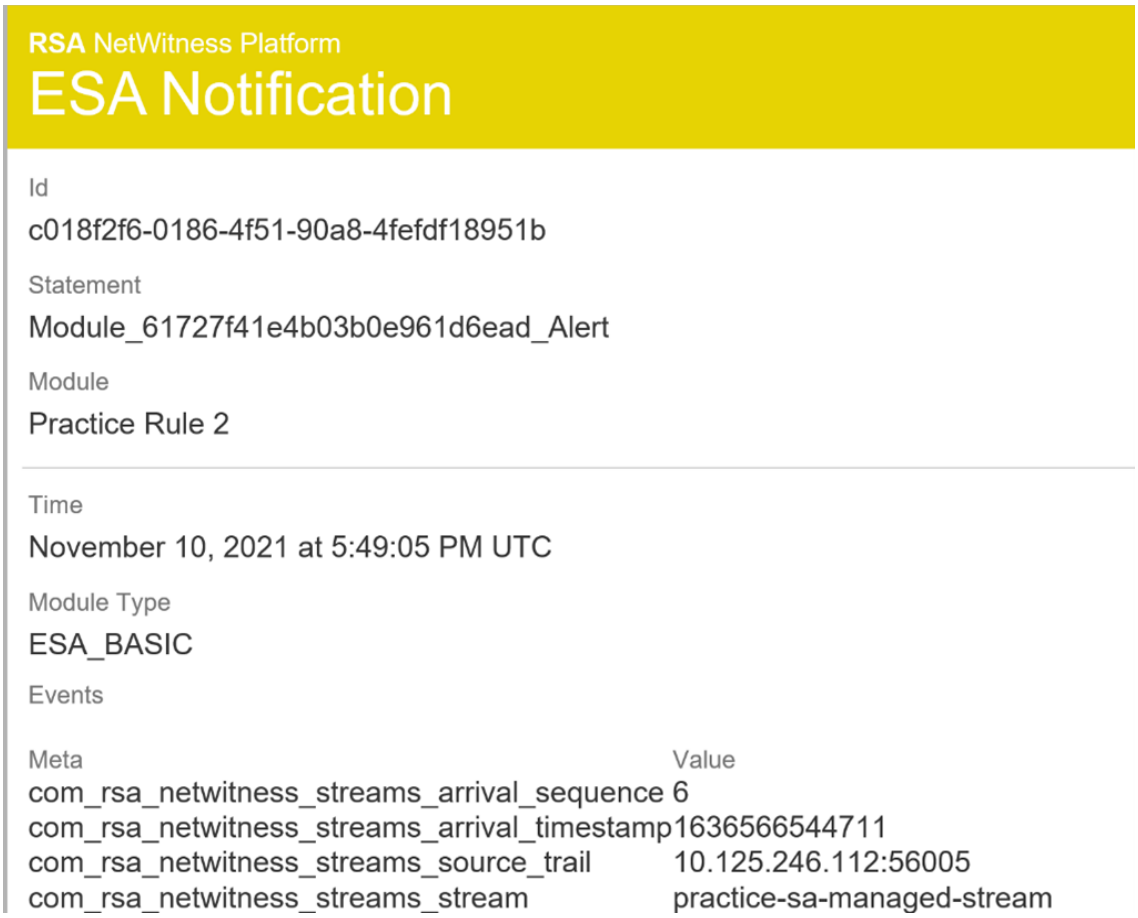
The following table describes the features in the Define Template dialog.

Field	Description
Name	Type a unique name for the notification template.
Template Type	Select the type of template that you want to create: • **Audit Logging**: Use this template for Global Audit Logging. • **Event Stream Analysis**: Use this template type for ESA alert notifications. • **Event Source Monitoring**: Use this template type for ESM notifications. • **Health Alarms**: Use this template type for Health and Wellness notifications. • **New Health and Wellness Alarms**: Use this template type for New Health and Wellness notifications.
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.

Field	Description
Template	Specify mandatory **CEF:** prefix when you create a template in CEF format. Define a Template for Global Audit Logging 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 Define a Template for ESA Alert Notifications. **Note:** Use Key references available in default notification templates.

Below is an example of a defined SMTP (email) template and output.





RSA NetWitness Platform

ESA Notification

Id

c018f2f6-0186-4f51-90a8-4fefdf18951b

Statement

Module_61727f41e4b03b0e961d6ead_Alert

Module

Practice Rule 2

Time

November 10, 2021 at 5:49:05 PM UTC

Module Type

ESA_BASIC

Events

Meta	Value
com_rsa_netwitness_streams_arrival_sequence	6
com_rsa_netwitness_streams_arrival_timestamp	1636566544711
com_rsa_netwitness_streams_source_trail	10.125.246.112:56005
com_rsa_netwitness_streams_stream	practice-sa-managed-stream

Output Tab

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

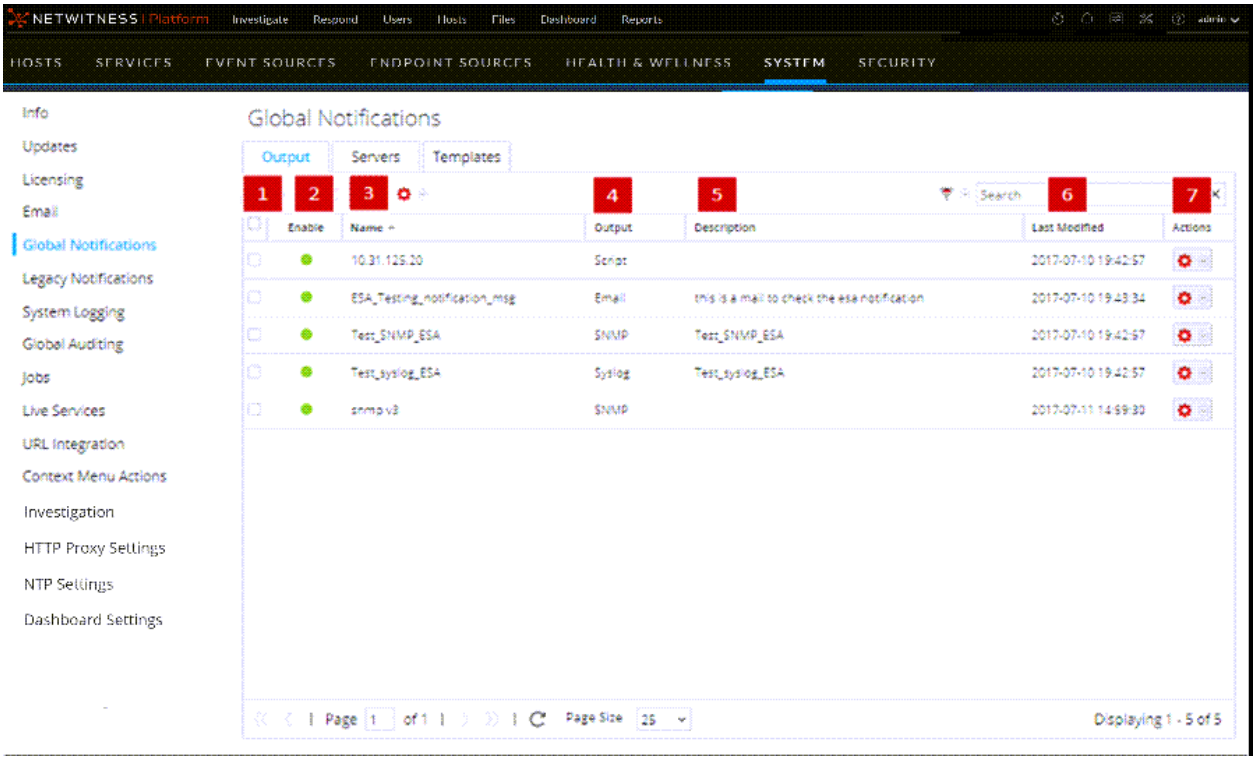
Role	I want to ...	Show me how
Administrator	Define notification outputs.	Configure Notification Outputs

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

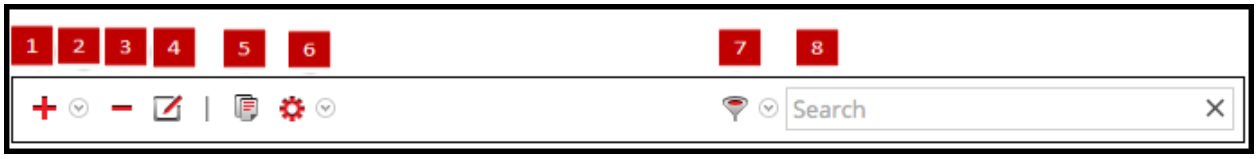
Quick Look

The following example illustrates Global Notification Outputs configuration.



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 you 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.

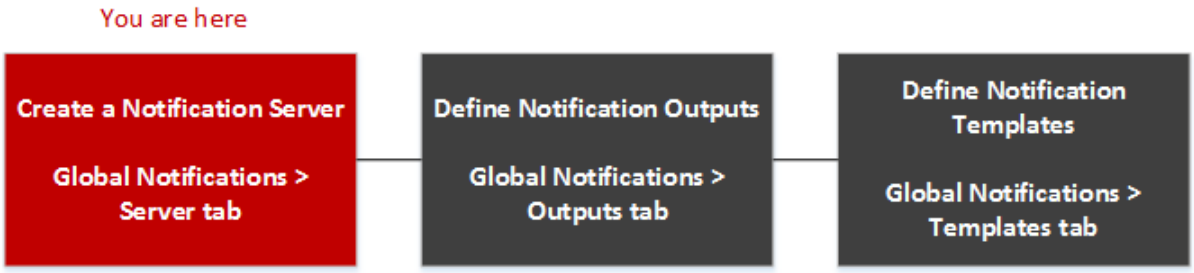
Configure **Notification Servers** in the Servers tab. On the Servers tab, add the servers from which you want to receive notifications from the system. For Global Audit Logging, define Log Decoders as Syslog Notification Servers.

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	Configure Notification Servers

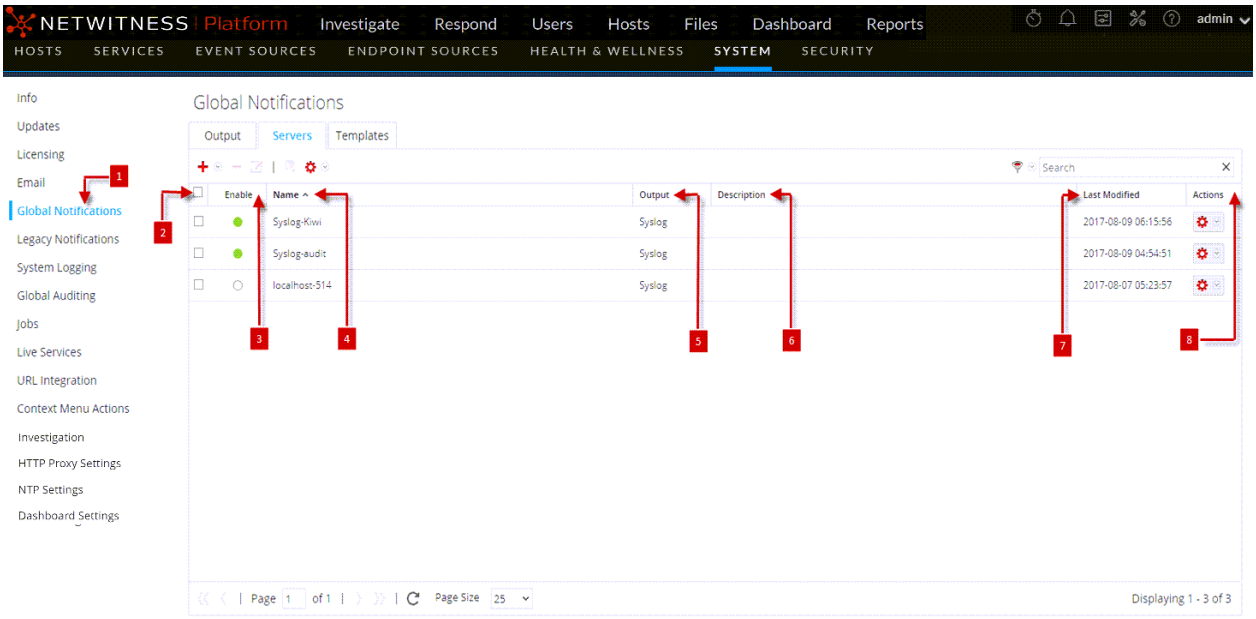
Related Topics

- 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

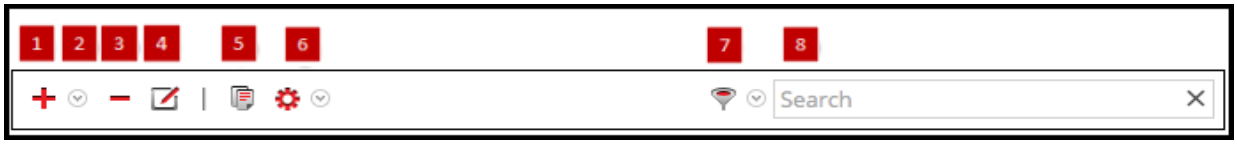
Quick Look

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.

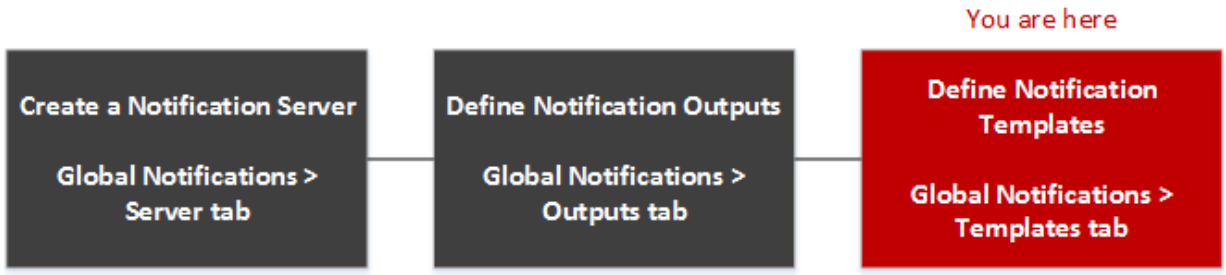
Templates Tab

The Notification Templates tab enables to configure notification templates. Global Notifications configurations define notifications settings for Event Source Management (ESM), Health and Wellness, New 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.

Workflow



What do you want to do?

Role	I want to ...	Show me how
Administrator	Define notification Templates	Configure Templates for Notifications

Related Topics

Configure Global Notifications Templates

Add a Template

Define a Template for ESA Alert Notifications

Delete a Template

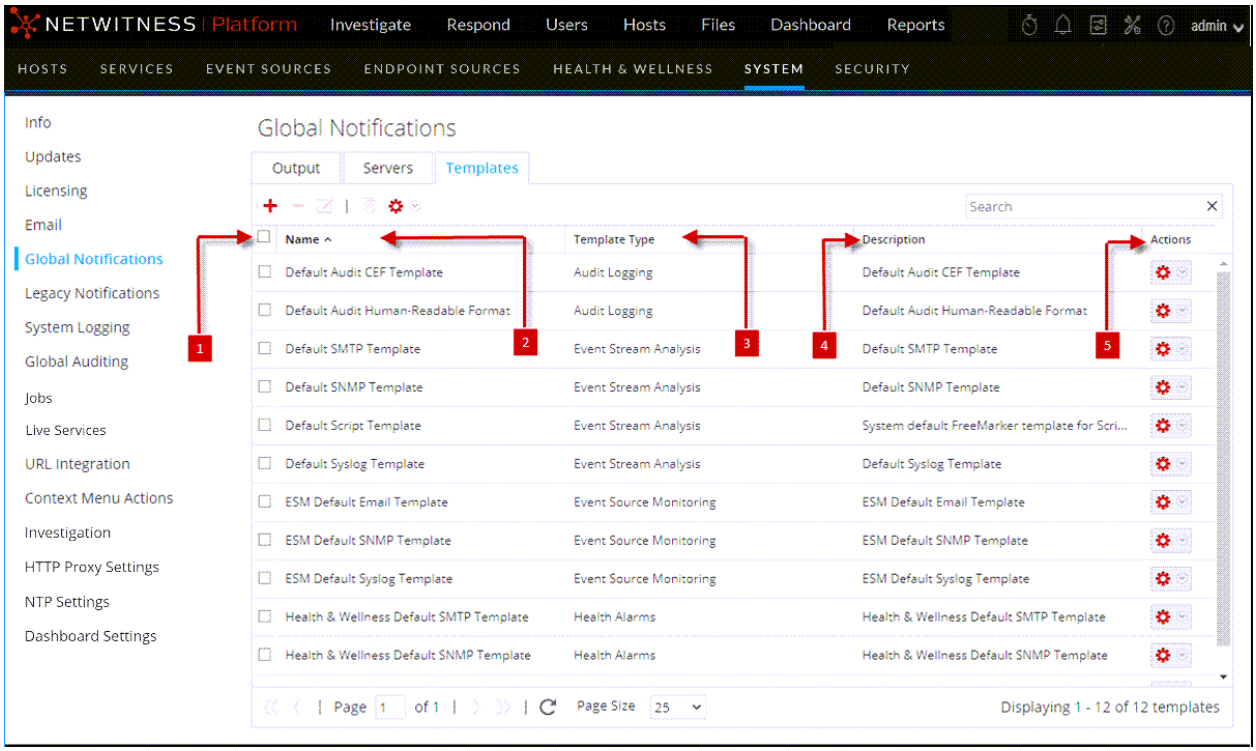
Duplicate a Template

Edit a Template

Import and Export a Global Notifications Template

Quick look

The following example illustrates Global Notification Templates Tab.



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 (Admin) > **System** > **HTTP Proxy Settings** panel.

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

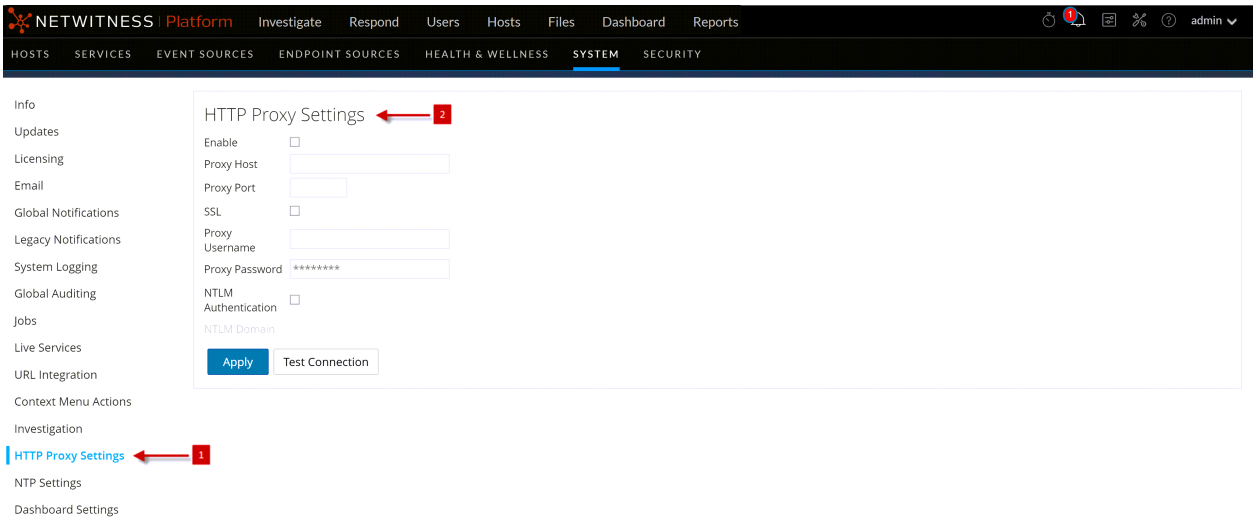
The HTTP Proxy Settings panel provides a user interface for configuring a proxy for use across NetWitness modules and services. The Proxy Settings set up a proxy to be used wherever a proxy is needed in NetWitness. The settings in this panel override any proxy settings configured for an individual service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

Related topics

"Configure Proxy for NetWitness Platform" in Additional Procedures

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 Sittings.

This table describes the features in the HTTP Proxy Settings section.

Feature	Description
Enable	Enable the system proxy configuration for use in NetWitness.
Proxy Host	The hostname for the proxy host.

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

Email Configuration Panel

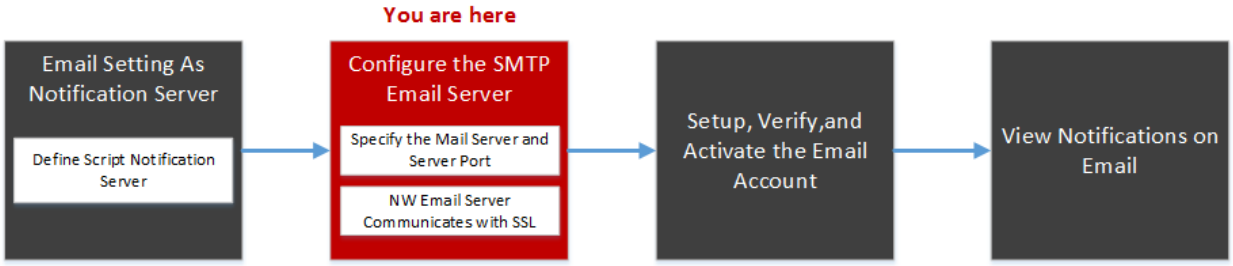
The Email Configuration Panel provides information about email configuration settings in the (Admin) > **System** > **Email Configuration** panel. NetWitness Platform sends notifications to users with email about various system events. To be able to configure these email notifications, first configure 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?

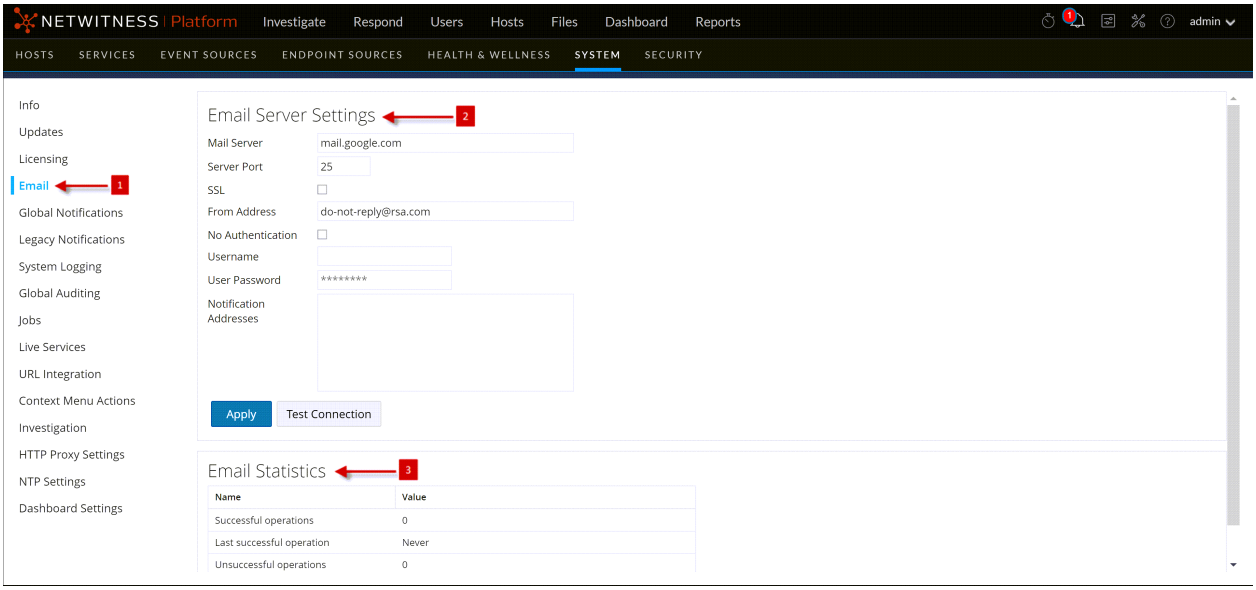
Role	I want to ...	Show me how
Administrator	Configure the SMTP Email Server	Configure Email Servers and Notification Accounts
Administrator	Email Setting as Notification Server	Configure the Email Settings as Notification Server
Administrator	Setup, Verify and Activate the Email Account	Receive Notification 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 sittings.
3 Provides feedback on Email operations.

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
Mail server	The email server name. The default value is **mail.google.com**.
Server port	The server port used to send and receive emails. The default value is **25**.
Use SSL	The preference for SSL use in communications between the email server and NetWitness. The default value is to not use SSL (unchecked).
From address	The address that appears in all emails from NetWitness. The default from address for emails is **do-not-reply@netwitness.com**.
Username	The username to access the email server. The default value is **blank**.
User password	The user password to access the email server. The default value is **blank**.

Feature	Description
Test connection	Tests the connection to the email server.
Apply	Applies the email configuration to this instance of NetWitness.

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.

Investigation Configuration Panel

The (Admin) > **System** > Investigation Configuration panel provides the user interface for administrators to configure the system-wide settings that NetWitness Investigate uses when analyzing data and reconstructing an event.

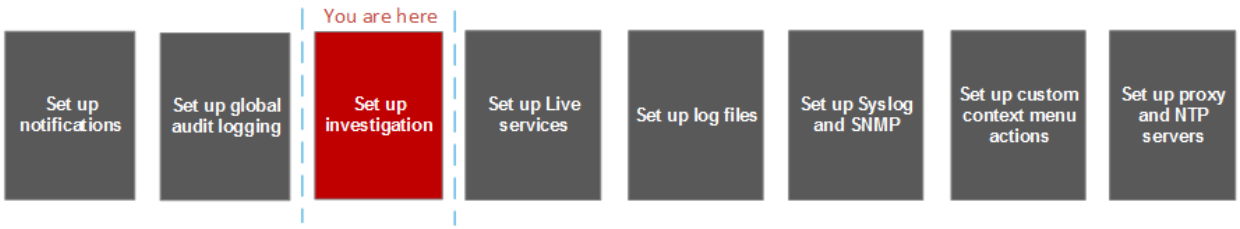
The settings allow an administrator to manage application performance for Investigate. As analysts analyze and reconstruct sessions that they are investigating, performance can be affected by operations that involve loading, searching, visualizing, and reconstructing large amounts of data.

Note: Analysts can also set individual preferences for Investigate in the Profiles view and in the Navigate, Legacy Events, and Events views.

To access the Investigation Configuration panel:

1. Go to **(Admin)** > **System.**
2. In the options panel, select **Investigation**.

Workflow



What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure Navigate, Legacy Events, and Events view settings	Configure Investigation Settings
Administrator	Map Context Hub Meta Types	Configure Investigation Settings
Administrator	Clear reconstruction cache for services	Configure Investigation Settings

Related Topics

- Standard Procedures

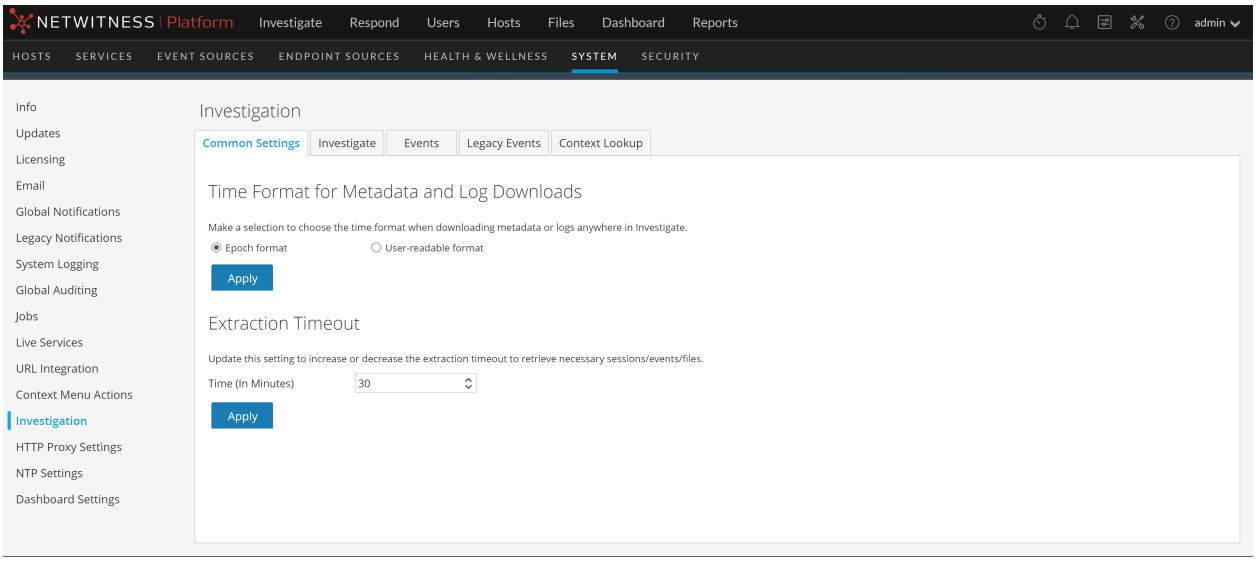
Quick Look

The Investigation Configuration panel has four tabs: Common Settings (Version 11.5 and later), Navigate, Events, Legacy 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.

Common Settings Tab

The Common Settings tab applies to all Investigate views.



The following table describes the options in this tab.

Parameter	Description
Time Format for Metadata and Log Downloads	
Epoch format	Use the Epoch format in downloads from Investigate (default value). These are Epoch representations of `2020-04-13 09:34AM`: • 12-hour representation = `61547519856000` • 24-hour representation = `61547519976000`

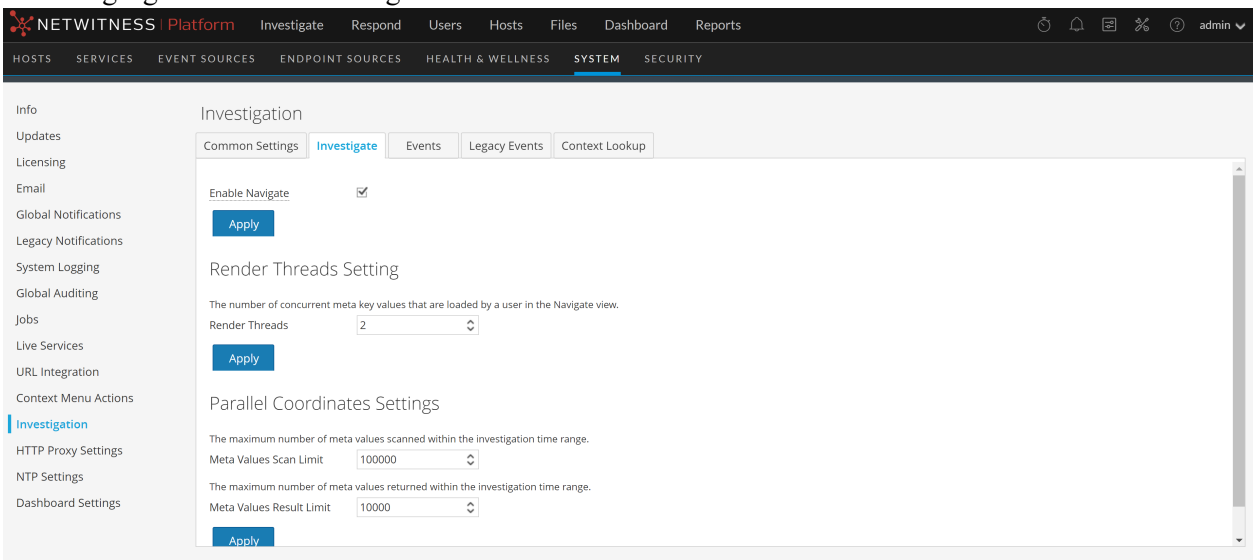
Parameter	Description

User-readable format	Use a user-readable time in downloads from Investigate. The downloads use a more understandable format that combines the user preference time zone, date format, and time format into an easily understood representation, which follows the industry standard ISO 8601 representation when possible.
	Examples of 12-Hour Format
	`04-13-2020T09:17:36AM-07:00`
	`13-04-2020T09:17:36AM-07:00`
	`2020-13-13T09:17:36AM-07:00`
	Examples of 24-Hour Format
	`04-13-2020T09:19:14-07:00`
	`13-04-2020T09:19:14-07:00`
	`2020-04-13T09:19:14-07:00`

Extraction Timeout	
Time (In Minutes)	Use this to set the time limit before the session expires when downloading the logs from the service.

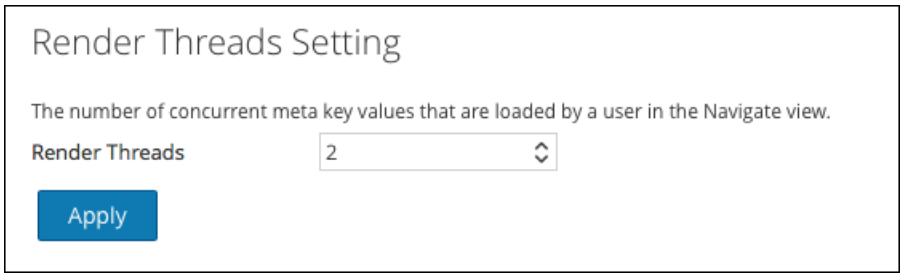
Investigate Tab

The Investigate tab has two sections: Render Threads Setting and Parallel Coordinates Settings. The following figure shows the Navigate tab.



Render Threads Setting

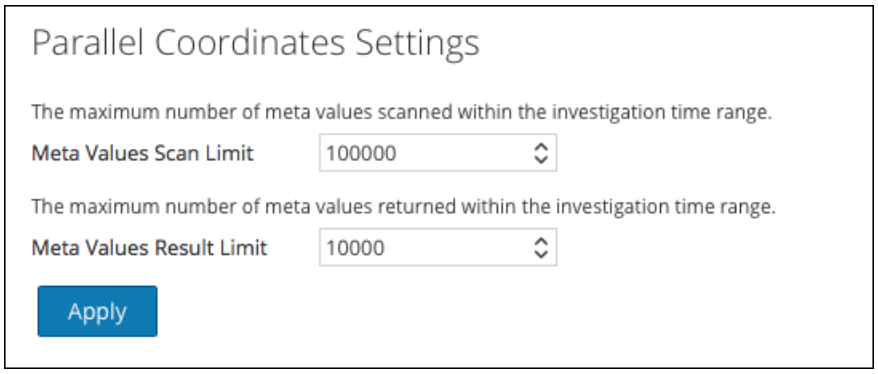
The Render Threads Setting is a selectable value between 1 and 20, which defines the number of concurrent (Values) loads in the Navigate view. The default value is 1.



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 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**.

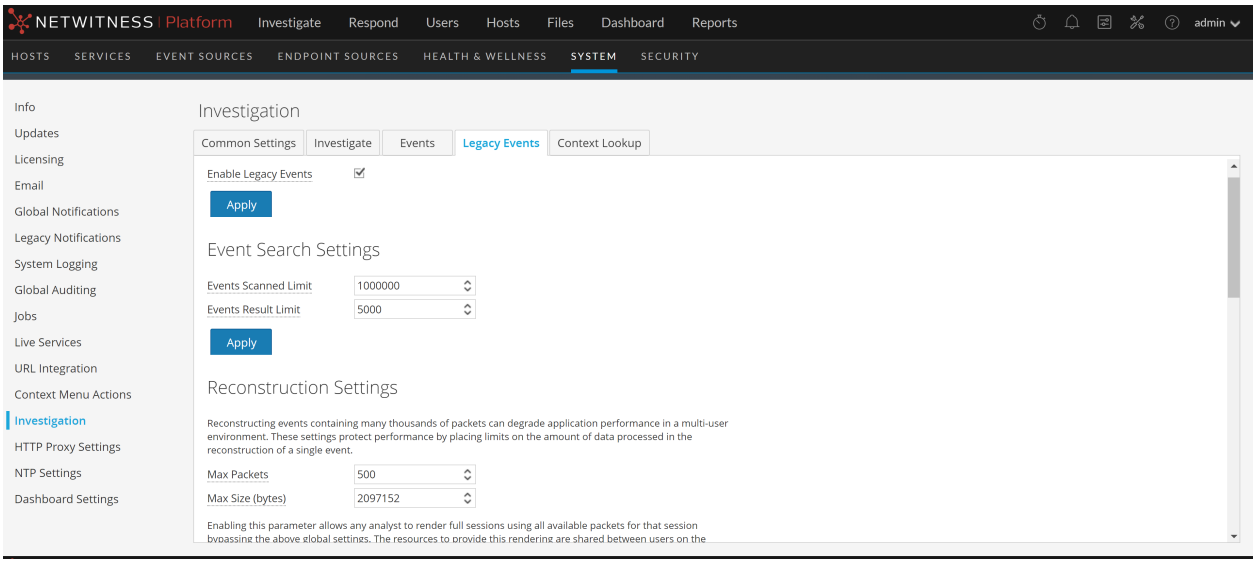


The following table describes the Parallel Coordinates Settings.

Parameter	Description
Meta Values Scan Limit	The maximum number of meta values scanned within the 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 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.

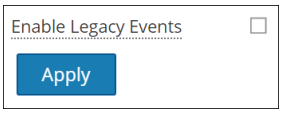
Legacy Events Tab

The Events tab provides configurable settings that affect the investigation of events. This tab has five sections: Enable Legacy Events, Event Search Settings, Reconstruction Settings, Web View Reconstruction Settings, and Reconstruction Cache Settings. The following figure shows the Events tab.



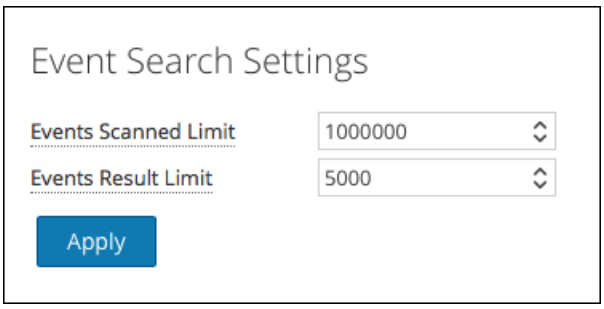
Enable Legacy Events

The Enable Legacy Events checkbox helps to enable and view the legacy events tab and view the classic events page on the UI. By default, this option is disabled.



Event Search Settings

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



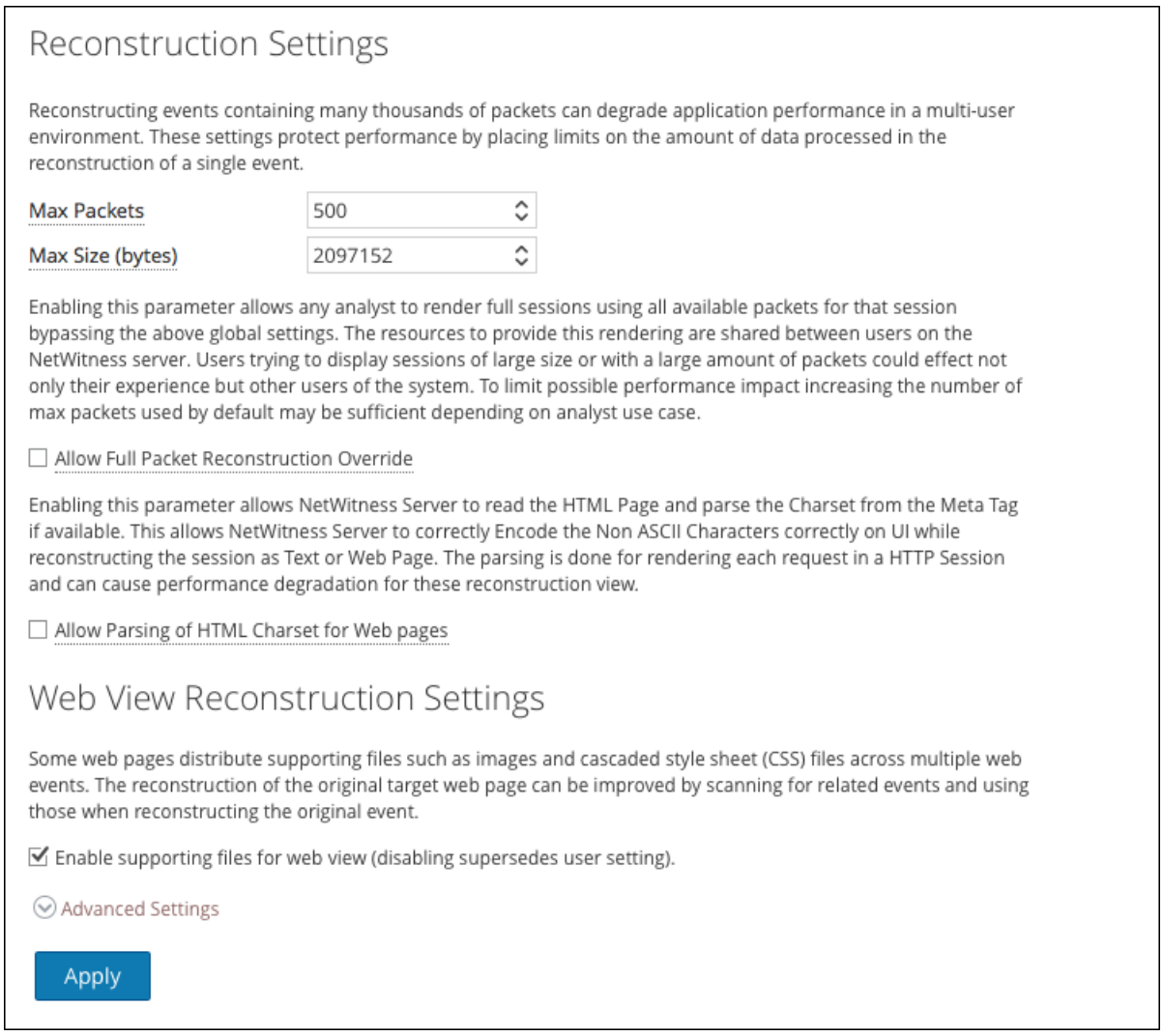
The following table describes the Event Search Settings.

Parameter	Description
Events Scanned Limit	The maximum number of events to scan when searching in the Events view. The actual number of events scanned may be slightly greater than the limit set here.
Events Result Limit	The maximum number of results to return when searching in the Events view. The actual number of results returned may be slightly greater than the limit here.

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).



The following table describes the Reconstruction Settings features.

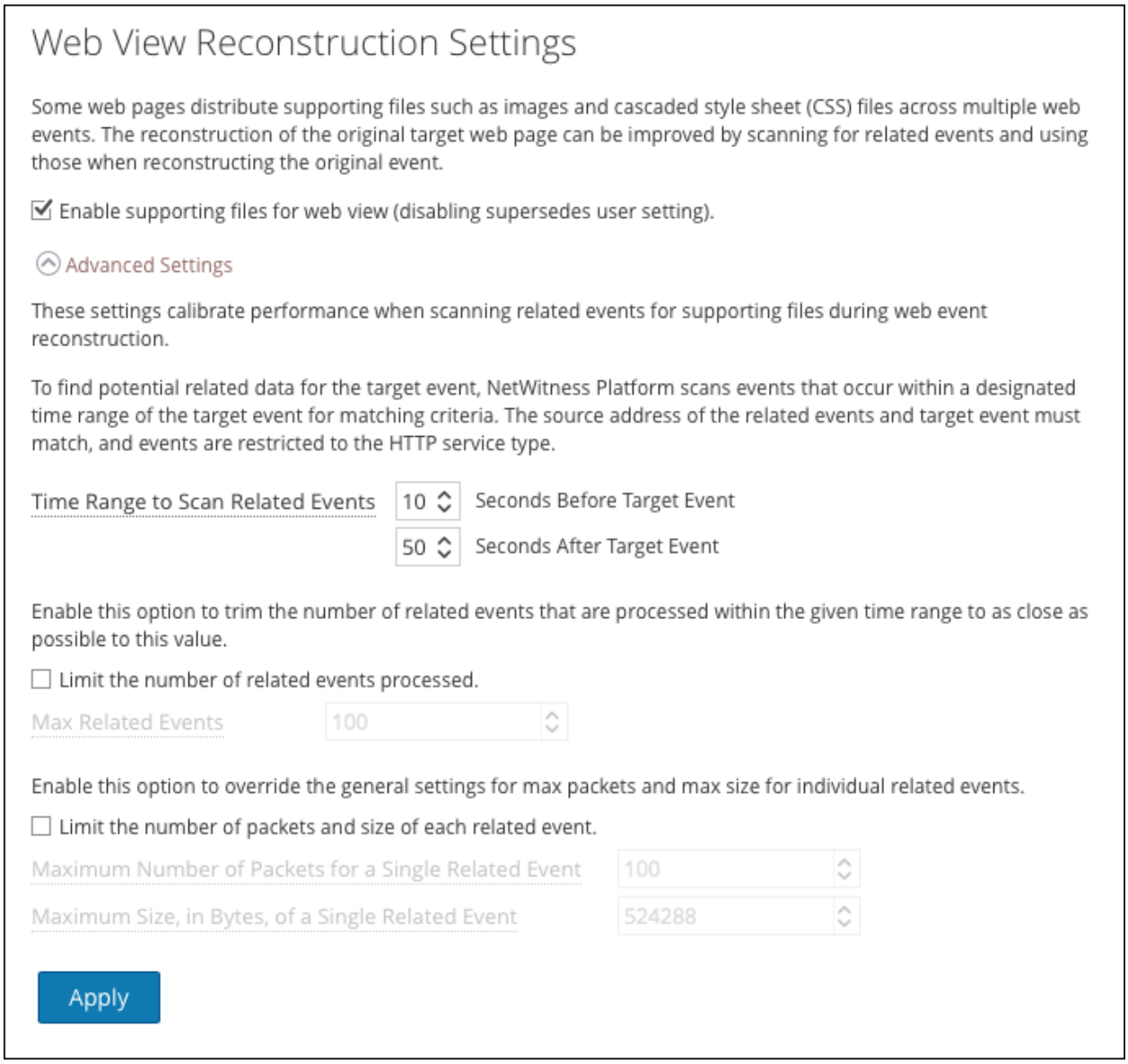
Parameter	Description
Maximum number of packets for a single event	This setting protects performance by placing a limit on the number of packets processed for a single event reconstruction. Possible values are in the range from 100 to 10,000 packets, using manual entry or increments of 100 from the selection list. The default value is 100 packets.
Maximum size, in bytes of a single event	This setting protects performance by placing a limit on the maximum size, in bytes, of a single event reconstruction. 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.
Allow Full Packet Reconstruction Override	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.
Allow Parsing of HTML Charset for Web pages	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.

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 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.



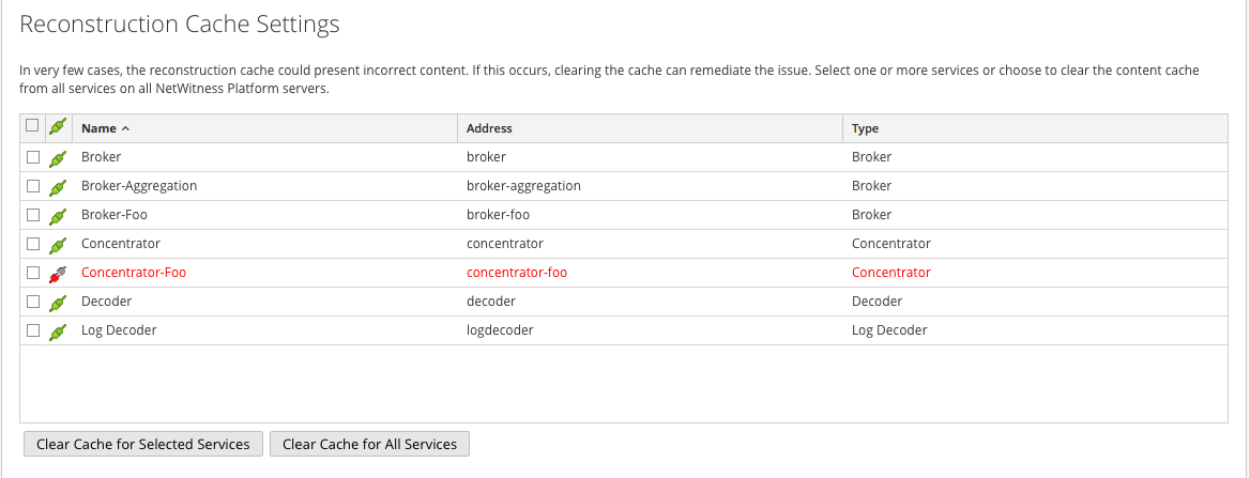
The following table describes the Web View Reconstruction Settings.

Parameter	Description
Enable supporting files for web view	This option determines how web views that have related data in other sessions are reconstructed. The default setting is enabled. 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. When disabled, supporting files from related events are not used and the setting for analysts to enable CSS use in reconstructions is disabled.

Parameter	Description
Time Range to Scan Related Events	Available when **Enable supporting files for web view** is checked. Configures the time range within which NetWitness 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. • Seconds Before Target Event • Seconds After Target Event
Limit the number of related events processed	Allows configuration of the maximum number of related events that NetWitness 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.
Max Related Events	When **Limit the number of events processed** is enabled, this field specifies the maximum number of related events that NetWitness scans within the specified time range to discover supporting files for the target event. This is a selectable value between 10 and 1,000, using an increment of 100. The default value is 100.
Limit the number of packets and size of each related event	Overrides the general settings for the maximum number of packets and maximum size (in bytes) for individual related events.
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 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.

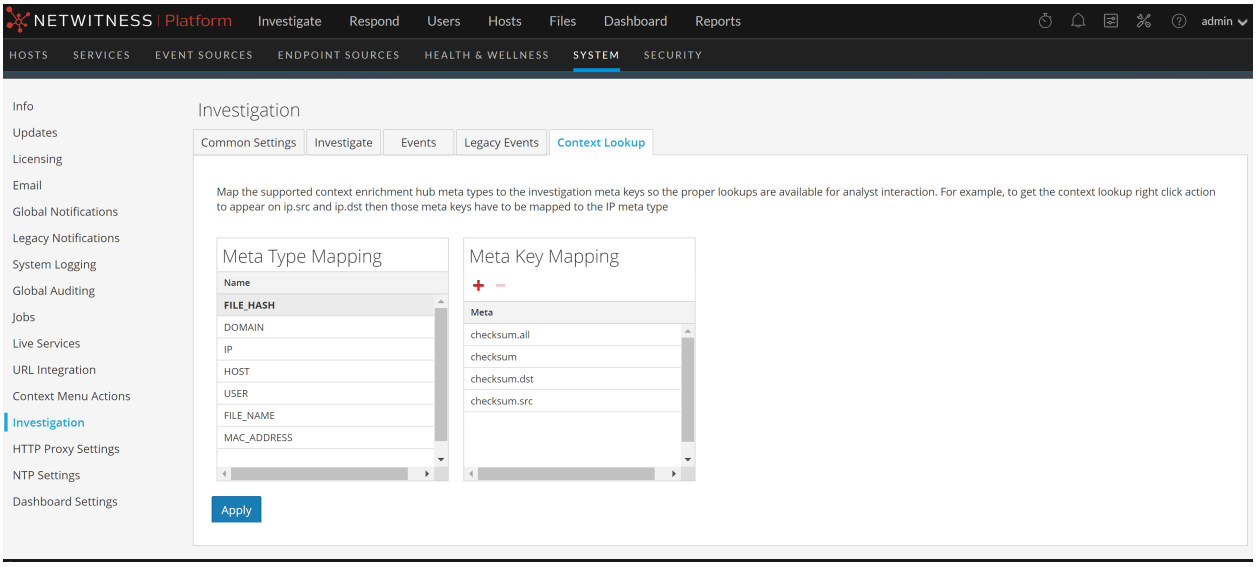


The following table describes the Reconstruction Cache Settings features.

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.
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.

Context Lookup Tab

Procedures associated with this panel are provided in "Manage Meta Type and Meta Key Mapping" in the *Context Hub Configuration Guide*. The following figure shows the Context Lookup tab.



The Context Lookup tab enables the administrator to configure the Investigate meta keys and meta type mapping. The administrator can add or remove meta keys found in Investigate to the list of meta types supported by Context Hub service. NetWitness Respond and Investigate use these default mappings for context lookup. For information about adding meta keys, see "Configure Context Hub Data Source Settings" in the *Context Hub Configuration Guide*.

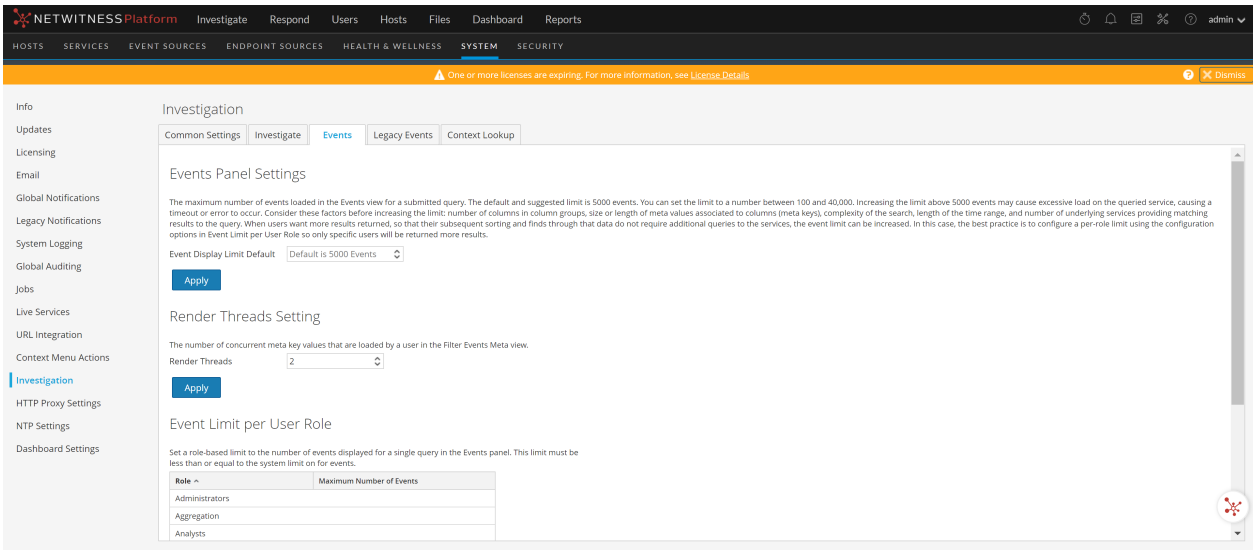
Caution: For the Context Lookup to work correctly in the Respond and Investigate views, this is the best practice: When mapping meta keys in the (Admin) > SYSTEM > Investigation > Context Lookup tab, add only meta keys to the Meta Key Mappings. Do not add fields in the MongoDB. For example, `ip.address` is a meta key and `ip_address` is not a meta key (it is a field in the MongoDB).

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

Feature	Description
	Adds a 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.

Events Tab

The following figure shows the Event tab.



The Events tab provides configurable settings that affect the number of events displayed in the Events panel. This tab has three sections: Events Panel Settings, Render Threads Setting, and Event Limit per User Role.

Feature	Description

Feature	Description
Event Display Limit Default	Specifies the maximum number of events loaded in the Events panel when a query is submitted. Possible values are integers between 100 and 40,000, and the default value is 5,000 events. If a query returns more events than the configured Event Limit Default, the Events panel title shows the analyst that more results are available but are not listed due to the limit. Increasing the limit may place additional load on the queried service; the ideal limit is determined by your environment.
Render Threads Setting	Specifies the maximum number of concurrent meta key values that are loaded by a single user in the Events Meta view. The default value is 1.
Event Limit Per User Role	Specifies the maximum number of events loaded for a single query for individual user roles. This limit must be less than or equal to the system events limit of 40,000, but it can be greater than the Event Display Limit Default.
Apply	Each setting has an Apply button, which saves the change. The change becomes effective immediately, and applies to any new queries submitted by users.

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, contact NetWitness Customer Support. 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

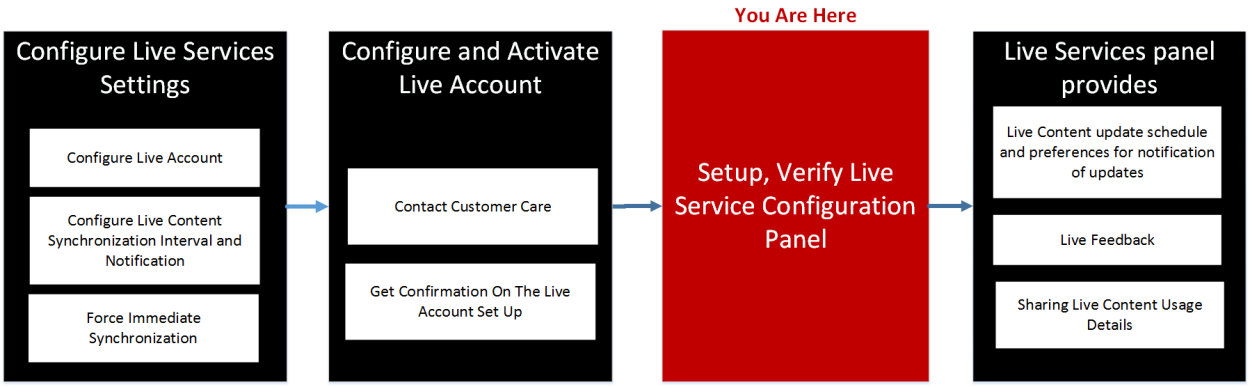
The Live Services panel provides the user interface for:

- The Live account
- The Live Content update schedule and preferences for notification of updates
- Participation in Live Feedback
- Sharing Live Content Usage Details

For information on Live Feedback, see Live Feedback Overview

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

Workflow



What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure Live Account, CMS Server Connection	Configure the Email Settings as Notification Server
Administrator	Upload Data to NetWitness for Live Feedback	Upload Data to NetWitness for Live Feedback

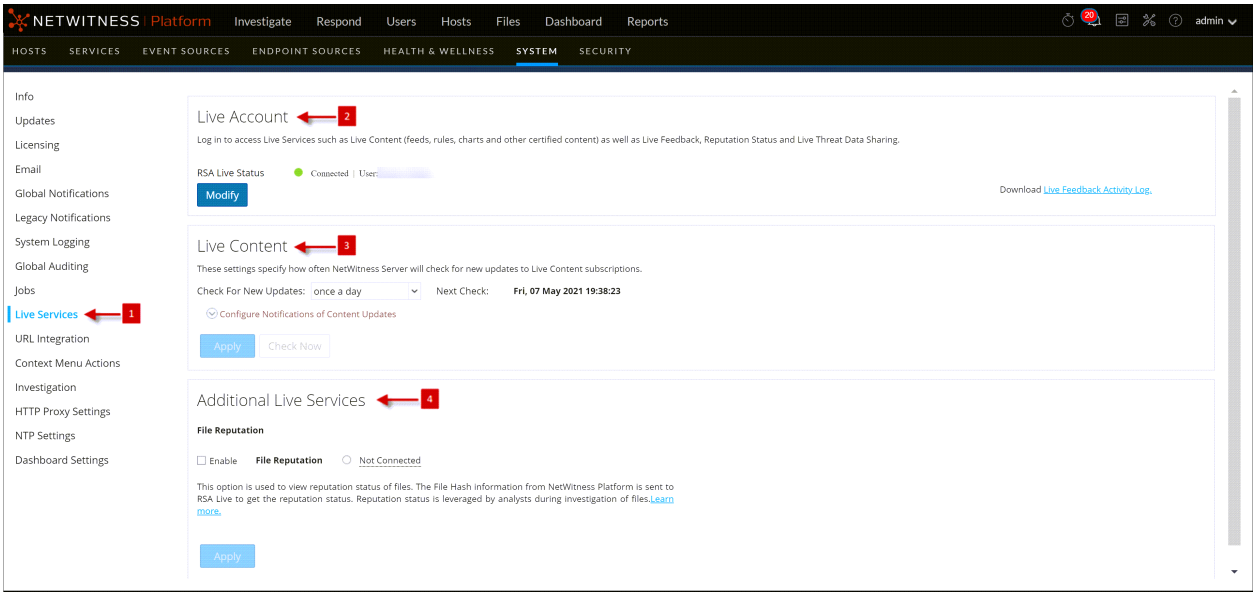
Role	I want to ...	Show me how
Administrator	Setup, Verify Live Service Configuration Panel	Live Services Configuration Panel
Administrator	Overview On Live Feedback	Live Feedback Overview

Related Topics

- Live Feedback Overview
- Configure Live Services Settings
- Upload Data to NetWitness for Live Feedback
- *Live Services Management Guide*

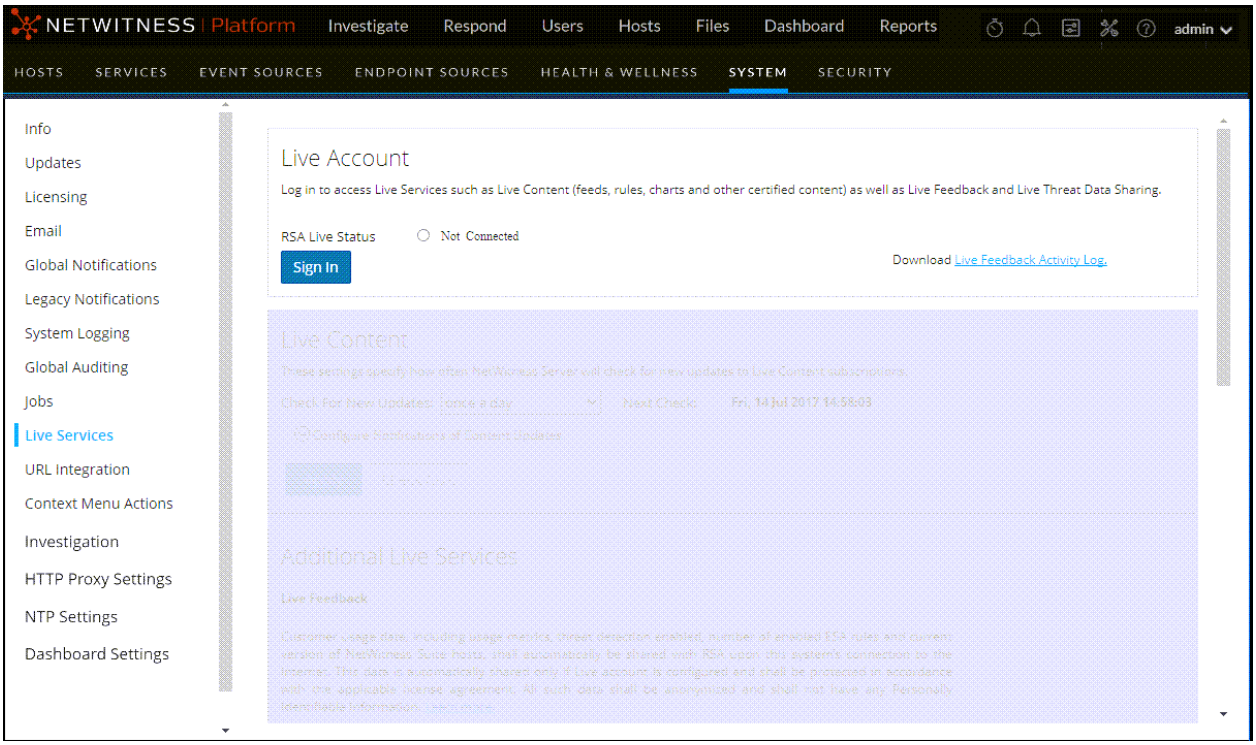
Live Services Quick Look

You access this view in the **(Admin)** > **System** > **Live Services**.



1 Displays the Live Services Configuration Panel.
2 Enter Live Account Credentials with the help of Customer Care.
3 Provides updates on Live Content.
4 Additional Live Services provide Live feedback.

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



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 NetWitness Content Management System. This information is provided by Customer Care.

The following table describes the Live Account section features.

Feature	Description
Host	The Live URL for the Content Management System. The default value points to the NetWitness CMS at **cms.netwitness.com**.
Port	The communications port for Live to send requests to the Content Management System. The default value for this field is **443**, which is the communications port on the Content Management System.
SSL	Allows the user to communicate via SSL.
Username	The Live account user name as provided by NetWitness Customer Support.
Password	The Live account user password as provided by NetWitness Customer Support.
Test connection	Tests if the connection is successful or not.
Apply	Saves and applies the configuration.

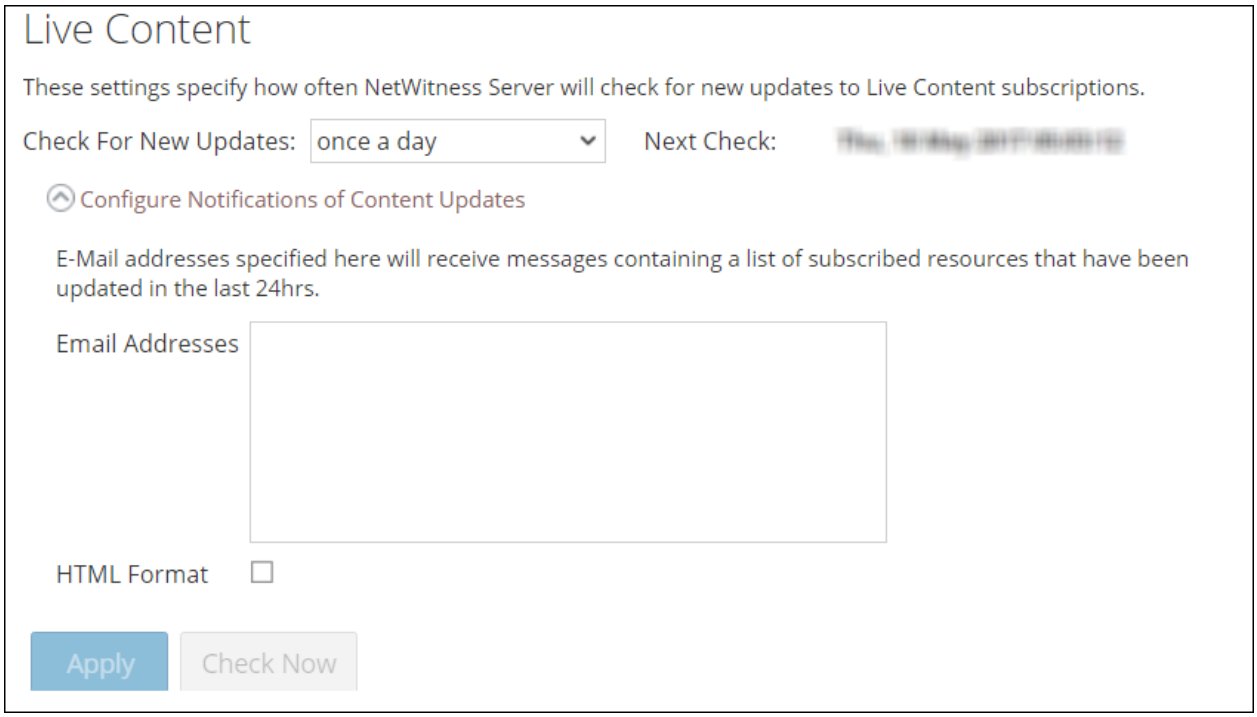
The Live Account section provides an option to download and share the Live Feedback historical data by clicking Live Feedback Activity Log.

For more information about how to download historical data, see Upload Data to NetWitness for Live Feedback

Live Content Section

You can configure the Live Content Synchronization interval and notification at which NetWitness 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**.



The following table describes the Live Content features.

Feature	Description
Check for new updates	This setting dictates how often NetWitness checks for new updates to Live Subscriptions and synchronizes subscribed resources and tags: • once a day • twice a day • four times a day • every hour • every other hour • every half hour The default value for this setting is once a day.
Next Check	Displays the time and date of the next scheduled Live synchronization based on the configured interval for checking.
Email Addresses	Email addresses specified here receive messages containing a list of subscribed resources that have been updated in the last 24 hours.
HTML format	Specifies the format of email messages. • Set = HTML • Cleared = text
Check Now	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. **Caution:** 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.
Apply	Applies the changed configuration to the subscription synchronization behavior. The changes become effective immediately. The **Next Live synchronization is scheduled for** field is updated if the time changed.

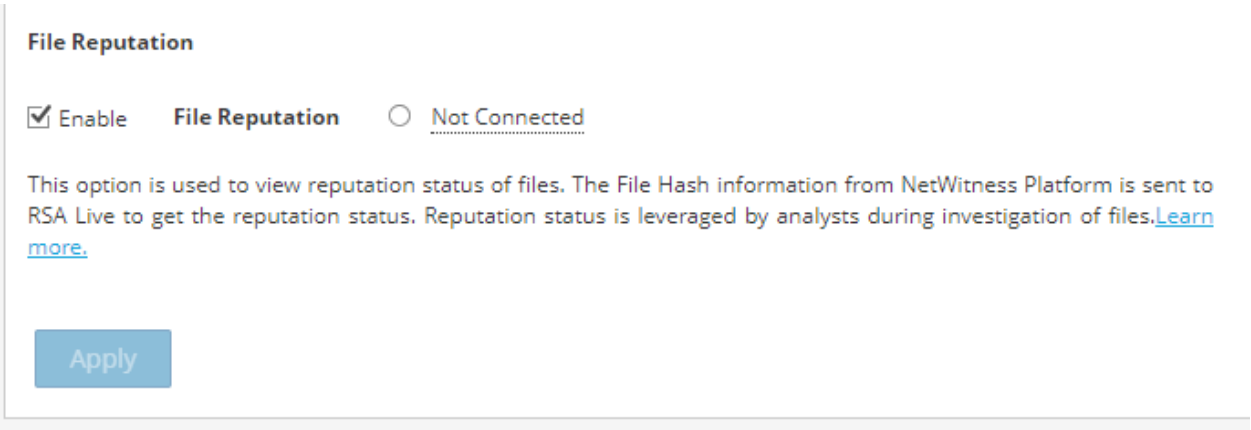
Force Immediate Synchronization

To force immediate synchronization, click **Check Now**. NetWitness 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. 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



Note: Click on Learn more to know more about the data NetWitness is collecting. For more information, see Live Feedback Overview

The following tables describes the Additional Live Services features.

Feature	Description

Live Feedback	Lists the types of data NetWitness is collecting:
	• Product Name
	• Product Version
	• Product Instance
	• Activation Key
	• Details of each Component such as:
	  • ID
	  • Name
	  • Version
	  • Instance ID
	• Metrics for each component

Additional Feedback Insights	Enables NetWitness to send anonymous, technical data about the content usage metrics to NetWitness. This option is enabled by default.

About Live Feedback Participation

Once you sign up for a Live account, Live Feedback automatically collects relevant information for further improvement and anonymously sends it to NetWitness. The shared data is protected in accordance with the applicable license agreement. For information on Live Feedback, see Live Feedback Overview. For information, see Configure Live Services Settings

If needed, you can manually download historical usage data and share it with NetWitness. For information on how to download historical usage data and share it with NetWitness, see Upload Data to NetWitness for Live Feedback.

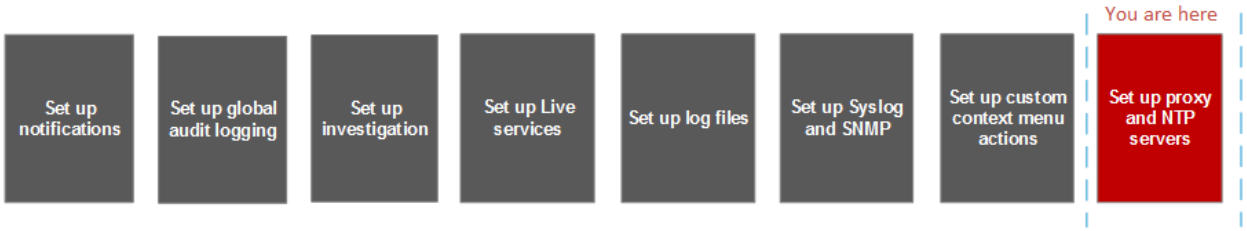
NTP Settings Panel

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

Note: NetWitness core hosts must be able to communicate with the NetWitness Server 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 uses NTP to synchronize the host machine clocks. You configure multiple NTP servers for Fail Over purposes.

Workflow



What you need to do?

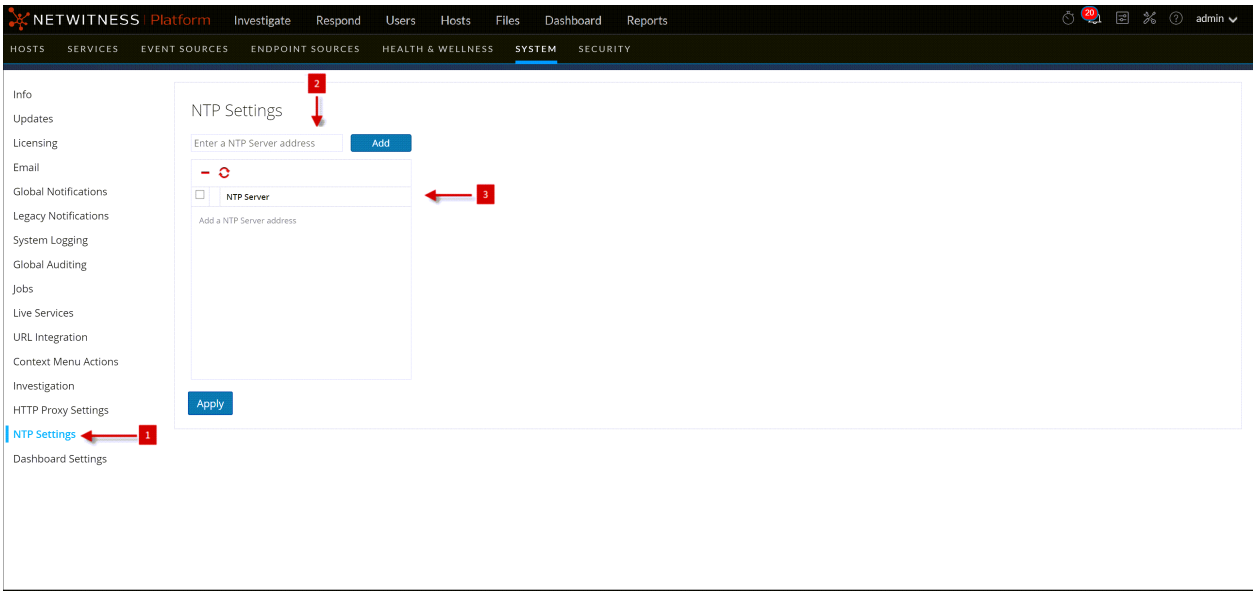
Role	I want to ...	Show me how
Administrator	Add or Modify an NTP Server	Configure NTP Servers

Related Topics

- Configure NTP Servers
- Troubleshoot Issues identified in the NTP Settings Panel or Log Files Messages

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.

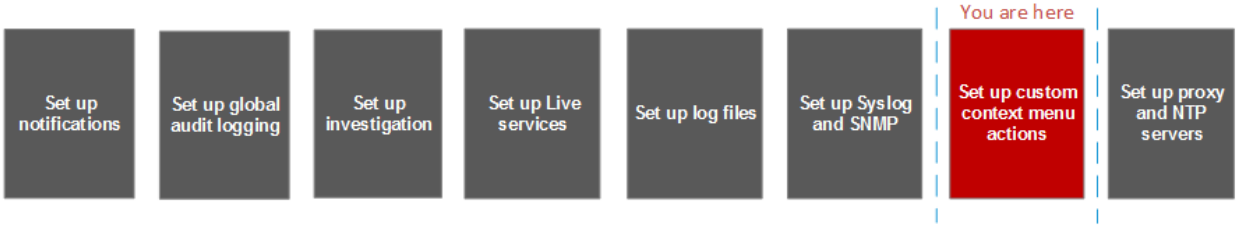
The following table describes the settings in the NTP Settings panel.

Setting	Description
Add	Enter the NTP Server IP Address or hostname to add the NTP server to NetWitness.
	Delete the selected NTP server.
	Synchronizes the selected NTP server.
	Selects the NTP server that you want to delete or synchronize.
NTP Server	NTP Server IP Address or hostname. If you click on an existing hostname, NetWitness makes the hostname editable and displays the following command buttons: • **Update** - Applies your edits. • **Cancel** - Cancels your edits.
Apply	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

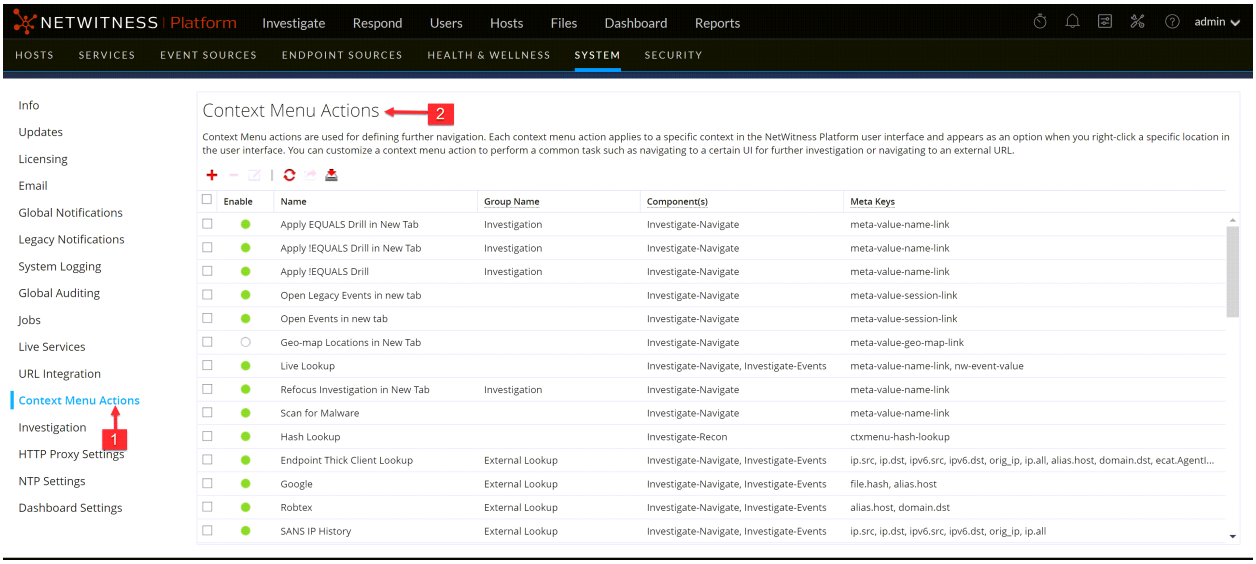


What do you want to do?

Role	I want to ...	Show me how
Administrator	Custom Context Menu Actions panel	Add Custom Context Menu Actions.

Quick Look

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



1 Displays the Context Menu Actions Panel.
2 Toolbar allows you to Add, Edit, Delete Context Menu Actions.

The Context Menu Actions panel has a list 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 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.
Visibility	Displays whether the context menu action is enabled or disabled.
Action Name	The name of the context menu action as it appears on the meta when a user right-clicks to initiate action.
Action Group	The action group under which this context menu action is grouped.
Component	The UI component to which the Action Name and Action Group belong.

Meta Keys	The names of the modules in which the context action is available. Currently all built-in context menu actions are for the Investigation module.
	When creating a context menu action, the parameter is `modules`.
	Here is a line of sample code:
	`"modules": [`
	`"investigation"`
	`],`

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.

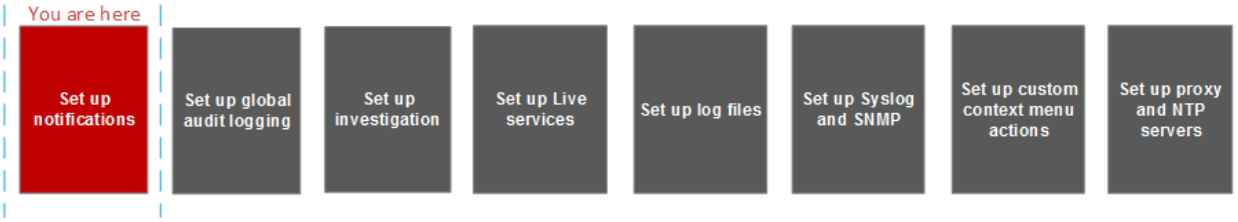
```
{
     "displayName": "User Agent String Lookup”, <!-- What name shows up in NW
UI -->
     "cssClasses": [
         “client”  <!-- What meta key to launch from -->
     ],
     "description": "",
     "type": "UAP.common.contextmenu.actions.URLContextAction",
     "version": "1",
     "modules": [
         "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



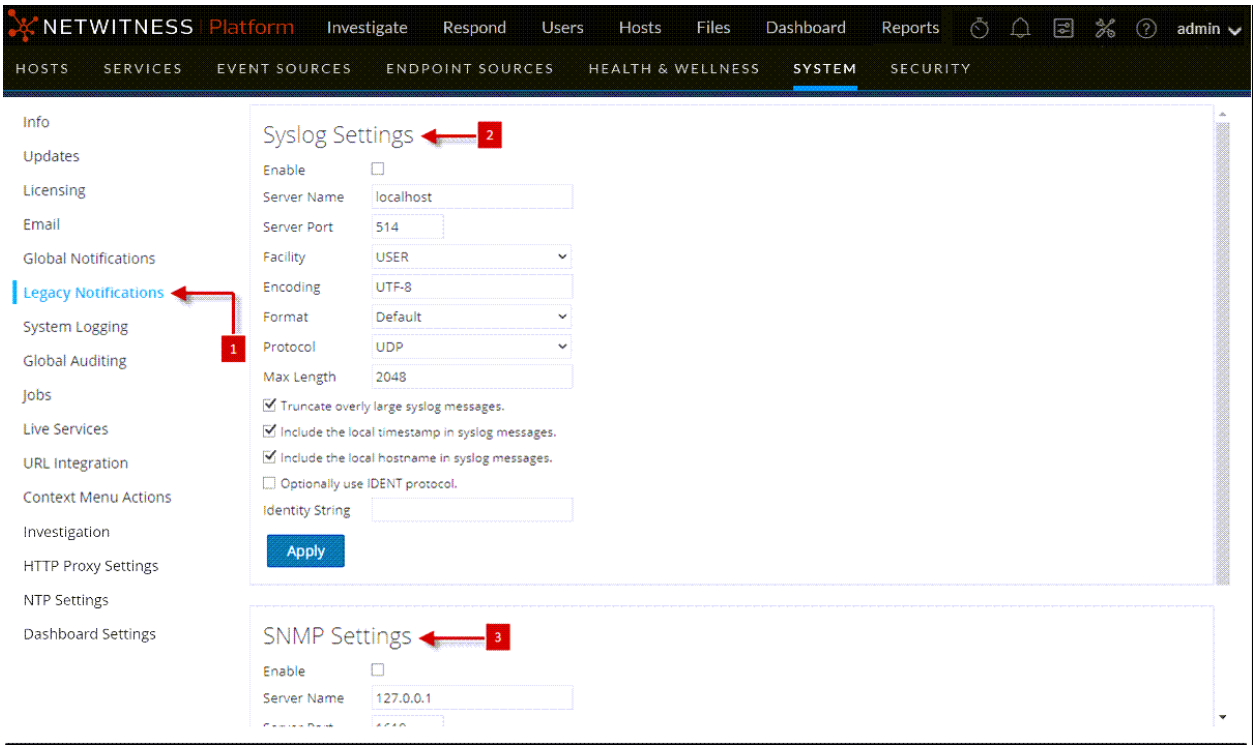
What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure Syslog Settings	Configure Syslog and SNMP Settings
Administrator	Configure SNMP Settings	Configure Syslog and SNMP Settings

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.

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
Enable	Enables the syslog settings configured here.
Server Name	Specifies the host where the target syslog process is running.
Server port	Specifies the port where the target syslog process is listening.

Feature	Description
Facility	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.
Encoding	Specifies the encoding to use for text in syslog messages, for example, UTF-8.
Format	Specifies the message format. Possible values are: Default, PCI DSS, or SEC.
Protocol	Specifies the communications protocol used when sending syslogs: UDP or TCP. By default, the UDP protocol is selected.
Max length	Specifies the maximum length in bytes of any syslog message. The default value is **2048**. Messages that exceed the maximum length are truncated when the **Truncate overly large syslog messages** checkbox is selected.
Truncate overly large syslog messages	When checked, any messages exceeding the maximum length are truncated.
Include the local timestamp in syslog messages	When checked, NetWitness includes the local timestamp in messages.
Include the local hostname in syslog messages	When checked, NetWitness includes the local hostname in syslog messages.
Optionally use IDENT protocol	When checked, NetWitness prepends the identity string to outgoing syslog alerts.
Identity string	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.
Apply	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
Enable	Enables the SNMP settings configured here.
Server Name	Specifies the SNMP trap host.
Server port	Specifies the listening port on the SNMP trap host
SNMP version	Specifies the SNMP version, **v1** or **v2c**.

Feature	Description
Trap OID	Specifies the object ID for the SNMP trap on the trap host that receives the audit event. The default value is **0.0.0.0.0.1**.
Community	Specifies the community string used to authenticate on the SNMP trap host, the default value is **public**.
Enable	Enables SNMP notifications as configured here.
Apply	Applies the SNMP configuration settings.