NetWitness® Platform

Version 12.5.1.0

Getting Started 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/.

November, 2024

Contents

Getting Started with NetWitness Platform

Overview

NetWitness is a powerful threat detection suite that enables Security Operation Centers (SOCs) to quickly locate, prioritize, and triage threats. NetWitness helps you to isolate and remediate known threats as well as those that were previously unknown. It provides deep insight into packets, logs, and endpoints that provide you with an unparalleled view into your enterprise or business.

NetWitness is powerful, but it is easier for Tier 1 Analysts to use because it automates the process of identifying and prioritizing suspicious threats. Tier 2 and Tier 3 Analysts can hunt for and locate threats by searching and filtering events and then examining events using reconstruction and analysis tools.

Architecture

NetWitness is a distributed and modular system that enables highly flexible deployment architectures that scale with the needs of the organization. NetWitness allows administrators to collect three types of data from the network infrastructure: packet data, log data, and endpoint data. The key aspects of the architecture are:

- **Distributed Data Collection**: The **Decoder** ingests packet data while the **Log Decoder** ingests log data. Decoders parse and reconstruct all collected network traffic from Layers 2 - 7, or log and event data from hundreds of devices and event sources, including NetWitness Endpoint data (if installed and configured). The **Concentrator** indexes metadata extracted from network or log data and makes it available for enterprise-wide querying and real-time analytics while also facilitating reporting and alerting. The **Broker** aggregates data captured by other devices and event sources. Brokers aggregate data from configured Concentrators; Concentrators aggregate data from Decoders. Therefore, a Broker bridges the multiple real-time data stores held in the various Decoder or Concentrator pairs throughout the infrastructure.
- **Real-time Alerting**: The NetWitness **Event Stream Analysis (ESA)** service provides advanced stream analytics such as correlation and complex event processing at high throughputs and low latency. It can process large volumes of disparate event data from Concentrators. ESA uses an advanced Event Processing Language (EPL) that allows analysts to express filtering, aggregation, joins, pattern recognition, and correlation across multiple disparate event streams. Event Stream Analysis helps to perform powerful incident detection and alerting.
- **Real-time Analytics** (automatic analysis of events): The Automated Threat Detection functionality includes preconfigured ESA analytics module for detecting Command and Control traffic.
- **NetWitness Server**: The NetWitness Server provides reporting, investigation, administration, and other aspects of the user interface.
- **Capacity**: NetWitness has a modular-capacity architecture enabled with direct-attached capacity (DACs) or storage area networks (SANs), that adapts to the organization's short-term investigation and long-term analytic and data-retention needs.

NetWitness provides large deployment flexibility. You can design its architecture using as many as multiple dozens of physical hosts or a single physical host, based on the particulars of the customer's performance and security-related requirements. In addition, the entire NetWitness system has been optimized to run on virtualized infrastructure.

The System Architecture comprises of these major components- Decoders, Brokers, Concentrators, Archivers, ESA, and Warehouse Connectors. NetWitness components can be used together as a system or can be used individually.

- In a security information and event management (SIEM) implementation, the base configuration requires these components- Log Decoder, Concentrator, Broker, Event Stream Analysis (ESA), and the NetWitness Server.
- In a forensics implementation, the base configuration requires these components- Decoder, Concentrator, Broker, ESA, Malware Analysis, and Endpoint Log Hybrid. The Respond Server service is also required and is used to prioritize alerts.

The table provides a synopsis of each major component:

System Component	Description
Decoder / Log Decoder	• NetWitness collects packet, log, and endpoint data. • Packet data, that is, network packets, are collected using the Decoder through the network tap or span port, which is typically determined to be an egress point on an organization's network. • A Log Decoder can collect four different log types - Syslog, ODBC, Windows eventing, and flat files. • Windows eventing refers to the Windows 2008 collection methodology and flat files can be obtained via SFTP. • Both types of Decoders ingest raw transactional data that is enriched, closed out, and aggregated to other NetWitness components. • The process for ingesting and parsing transactional data is a dynamic and open framework.
Endpoint Log Hybrid	• Collects and manages endpoint (host) data from Windows, Mac, or Linux hosts. • Records data about every critical action, such as process, file, registry modification, network connections, and user console interactions. • Collects Windows logs and file logs from Windows host, if configured. • Generates metadata to correlate endpoint data with sessions from other events sources, such as logs and network. • Performs on-demand memory analysis and suspicious user behavior detection.

System Component	Description
Concentrator	• Provides index and query capability to NetWitness Collections. • Can optionally forward data to ESA.
Broker	• Distributes NetWitness Collection access across many Concentrators or Archivers, making the entire NetWitness enterprise appear as a single collection.
Archiver	• The Archiver service enables long-term log archiving by indexing and compressing log data and sending it to archiving storage. • The archiving storage is optimized for long-term data retention, and compliance reporting. • Archiver stores raw logs and log metadata from Log Decoders for long-term retention, and it uses Direct-Attached Capacity (DAC) for storage. **Note:** Raw packets and packet metadata are not stored in the Archiver.
Event Stream Analysis (ESA)	• ESA provides event stream analytics such as correlation and complex event processing at high throughputs and low latency. It can process large volumes of disparate event data from Concentrators. • ESA uses advanced Event Processing Language that allows users to express filtering, aggregation, joins, pattern recognition, and correlation across multiple disparate event streams. • ESA helps to perform powerful incident detection and alerting.

Core Versus Downstream Components

In NetWitness, the Core services ingest and parse data, generate metadata, and aggregate generated metadata with the raw data. The Core services are Decoder, Log Decoder, Concentrator, and Broker. Downstream systems use data stored on Core services for analytics; therefore, the operations of downstream services are dependent on Core services. The downstream systems are Archiver, ESA, Malware Analysis, Investigate, and Reporting.

Although the Core services can operate and provide a good analytics solution without the downstream systems, the downstream components provide additional analytics. ESA provides real-time correlation across sessions and events as well as between different types of events, such as log, packet, and endpoint data. Investigate provides the ability to drill into data, examine events and files, and reconstruct events in a safe environment. The Malware Analysis service provides real-time, automated inspection for malicious activity in network sessions and associated files.

Logging in to NetWitness Platform

Note: NetWitness supports modern (or current) versions of Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari. It is possible to use a different browser, but some features may not function as expected. Internet Explorer is no longer supported.

Logging in to NetWitness can vary based on your environment. You may have an internal user account or an external user account. Internal user accounts are local to the NetWitness and internal users can log in to NetWitness and receive role-based permissions. External user accounts authenticate outside of the NetWitness and are mapped to NetWitness roles. If you are an external user and you cannot access NetWitness or view the information that you need, contact your System Administrator. Your Administrator can assign the appropriate roles to your account.

NetWitness Platform also supports Single Sign-On authentication (SSO) using Security Assertion Markup Language 2.0 (SAML 2.0) protocol with Active Directory Federation Services (ADFS) as the Identity Provider.

If SSO authentication is enabled by your administrator, you will be redirected to the Identity Provider User Interface instead of the default NetWitness login page. After you enter the username and password you will be securely logged into NetWitness Platform.

Note: Single Sign-On (SSO) authentication can be used to access the NetWitness Platform UI, and Analyst UI Deployment.

1. Use the icon provided by your Administrator, or type the following in your web browser:
   `https://<hostname or IP address>/login`
   Where `<hostname or IP address>` is the hostname or the IP address of your NetWitness server.
   If Single Sign-On authentication is enabled, this redirects you to the ADFS login screen.
2. Enter the username and password, and then click **Sign in**.
   If the login is successful, you will be logged into the landing page specified in the user preferences.

Note: If you had previously authenticated to any other application configured to the same IDP, then you may be redirected to the requested NetWitness Platform UI without being prompted for the credentials.

If you are locked out

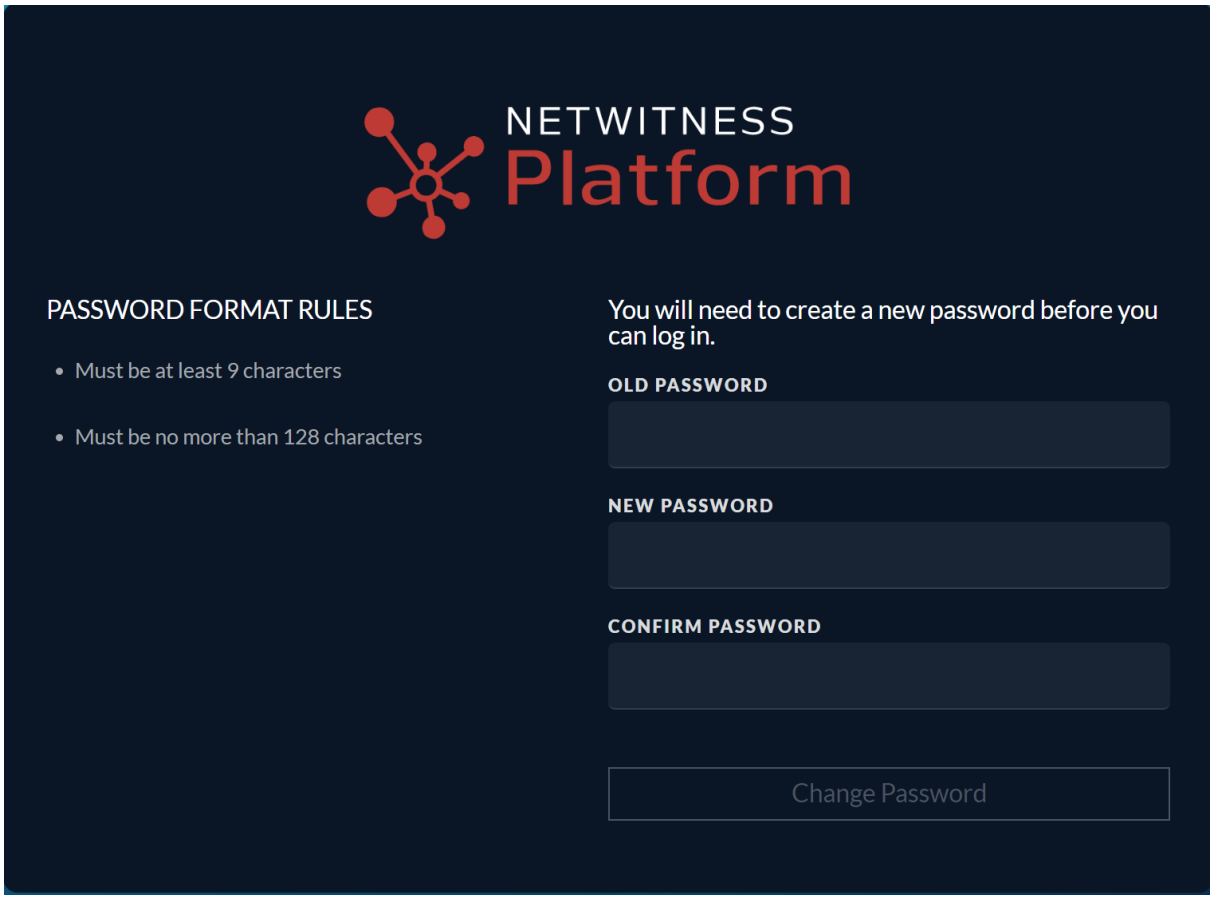
Note: This information applies to internal accounts only. It does not apply to Active Directory or PAM accounts.

If you try too many times to log in with an incorrect username or password, your account will be locked. Contact your Administrator to unlock your account.

If you have a new account or your account is expired

Note: This procedure applies to internal accounts only. It does not apply to Active Directory or PAM accounts.

1. In the dialog to create a new password, enter your old password, type a new password, and confirm it. Password format rules (as defined by your system administrator) are provided on the left and your new password must conform to the indicated format rules.



2. Click **Change Password**.

If you do not have the appropriate access to NetWitness

If you are able to log in successfully, but you are not able to view the information that you need, it is possible that you need a user role assigned to your user account. Contact your NetWitness Administrator for assistance.

Log Off NetWitness Platform

To log off from the Respond and some Investigate views

1. In the main menu bar, select your username, for example, admin.
2. In the User Preferences, click **Sign Out**.

To log off from the other views

In the main menu bar, select your username and then select **Sign Out**.

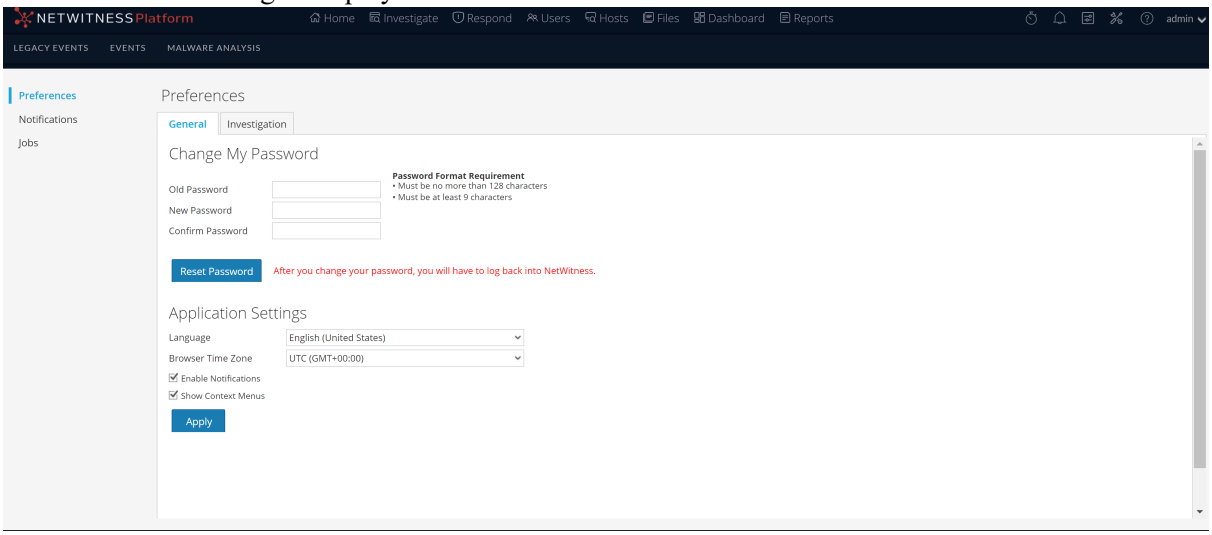
Changing Your Password

You can change the password that you use for NetWitness authentication at any time in your user preferences. Your administrator defines the appropriate password strength requirements for your NetWitness password, such as minimum password length and minimum number of uppercase, lowercase, decimal, non-Latin alphabetic, and special characters. These requirements are then displayed when changing your password.

To change your password:

1. Do one of the following:
   - For most views, such as Investigate, Dashboard, Reports, (Configure) or (Admin) , select your username, for example admin, and then select **Profile**.
   - In the Springboard, Investigate view (Events), Respond, Users, Hosts, and Files, select your username, for example admin, and in the User Preferences dialog click **Change my password**.

   The Preferences dialog is displayed.



2. In the **Change My Password** section, enter the password that you used to authenticate to NetWitness in the **Old Password** field.
3. In the **New Password** field, enter the password that you want to use for the next login.
4. In the **Confirm Password** field, retype the new password.
5. Click **Reset Password**.
   You will be logged out of NetWitness for the changes to take effect. The new password becomes effective the next time you log in to NetWitness.

For more information on user preferences, see Setting User Preferences.

Identifying Your Role

The roles listed here are the typical roles or functions of a Security Operations Center (SOC). Determine the role or roles that you perform in the SOC. You can use these functions as a guide to decide how to set up and navigate NetWitness so that you can efficiently perform your job tasks.

SOC Team

SOC Manager
(SOC Management and Reporting)

- Manage SOC readiness
- Respond to incidents
- Respond to data breaches

Data Privacy Officer

- Monitor and protect privacy and sensitive information

Incident Responder
(T1 Analyst)

- Respond to incidents
- Remediate incidents

Threat Hunter
(T2/T3 Analyst)

- Hunt for threats
- Conduct forensic analysis
- Recommend issues for remediation
- Remediate issues

Content Expert
(Threat Intelligence)

- Investigate new threat intelligence
- Evaluate and create new feeds
- Create correlation rules to flag indicators of compromise

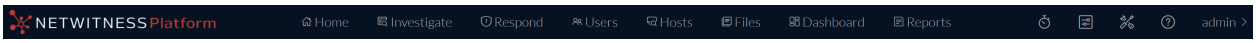
System Administrator

- Install and configure equipment and software
- Manage user access
- Monitor and fine tune performance
- Backup and restore data
- Manage storage and archives
- Update software
- Create reports for regulatory compliance

NetWitness Platform Basic Navigation

The NetWitness application is divided into Eleven main functional areas, known as views, that are based on typical Security Operation Center (SOC) roles.

Note: On upgrade to version 12.5 or later, by default the **Home** page is displayed if you have not configured the default landing page in previous versions.



- **Home**: NetWitness introduces a new Home page menu that consists of **Admin**, **Analyst**, and **Manager** views. Each home page is comprised of multiple widgets. Administrators, Analysts, and SOC Managers can access the respective widgets that display certain data in graphical form. The data can be associated with Endpoints, Users, Assets, Content, Incidents, Alerts, MITRE ATT&CK, Retention, and many more.
- **Springboard**: Springboard presents Analysts with the platform-wide detections and signals in a single view to hunt and investigate faster than ever before. System Administrators set up and maintain the Springboard. You can view the Springboard at any time by clicking NetWitness in the main menu. For more information, see Managing the Springboard.
- **Investigate**: This view is primarily for Threat Hunters, who prefer to manually hunt for threats using NetWitness metadata, raw event data, and event reconstruction and analysis. Incident Responders also use this view to get details about events associated with an incident being investigated. Both Threat Hunters and Incident Responders can use the forensic event reconstruction and event analysis features in this view.
- **Respond**: This view is for Incident Responders, who can view a list of prioritized incidents to triage. These incidents come from sources such as ESA rules, NetWitness Endpoint, or ESA Analytics modules for Automated Threat Detection. You can also view all of the alerts received by NetWitness here.
- **Users**: This view is for SOC Managers and Analysts to discover, investigate, and monitor risky behaviors across entities namely Users and Network in your environment.
- **Hosts**: This view is for Analysts, who can investigate or perform analysis on hosts using attributes such as IP address, host name, Mac address, risk score, and so on.
- **Files**: This view is for Analysts, who can investigate or perform analysis on files using attributes such as IP address, host name, Mac address, risk score, and so on
- **Dashboard**: This view is for all users. You can view dashboards on different areas of interest depending on your user permissions.
- **Reports**: This view is for all users. You can view reports on different areas of interest depending on your user permissions.
- **Configure**: This view is for Threat Intel personnel (Content Experts), who configure data sources and inputs to NetWitness. Content Experts use this area to download and manage Live content. They

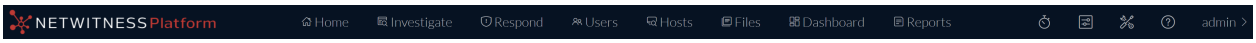
can also create and manage incident and ESA rules.

- **Admin**: This view is for System Administrators, who set up and maintain the overall application.

Accessing Main Views

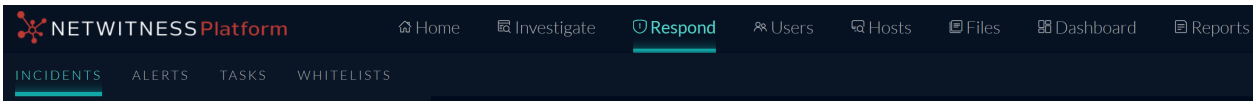
The options that open each of the main views are listed at the top of the browser window. With the appropriate permissions, you can access any of these views at the top of every UI at any time.

Note: Home page is newly introduced in NetWitness 12.5 version .



Secondary Menus

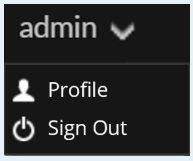
The main views have secondary menus with additional views that you can select, which vary according to the tasks that you can complete. The following example shows the Respond menu.



Additional Options

In addition to the main views, there are additional options at the top of the UI that are common to the application.

The following table describes the common options.

Common Option	Name	Description
	Jobs	In the Investigate, Dashboard, Reports,  (Configure) , and  (Admin) views, click this icon to view and manage your jobs in the Jobs tray. Jobs are on-demand or scheduled tasks that take some time to complete in the NetWitness application.
	Notifications	Click this icon to view notifications from the application.
	User Preferences	Click this icon to view your available user preference options. You can manage your user preferences and log out of NetWitness.
	User Profile	Click your user profile to view the available options. You can manage your user preferences, change your password, and log out of NetWitness UI.

Common Option	Name	Description
	Help	Click this icon to view NetWitness help topics.

Main Views

The following sections explain the main views:

- Home
- Springboard
- Investigate
- Respond
- Users
- Hosts
- Files
- Dashboard
- Reports
-  Configure
-  Admin

Home

(From 12.5 and later) NetWitness Platform introduces a new **Home** page menu that consists of **Admin**, **Analyst**, and **Manager** views. Each home page is comprised of multiple widgets. Administrators, Analysts, and SOC Managers can access the respective widgets that display certain data in graphical form. The data can be associated with Endpoints, Users, Assets, Content, Incidents, Alerts, MITRE ATT&CK, Retention, and many more.

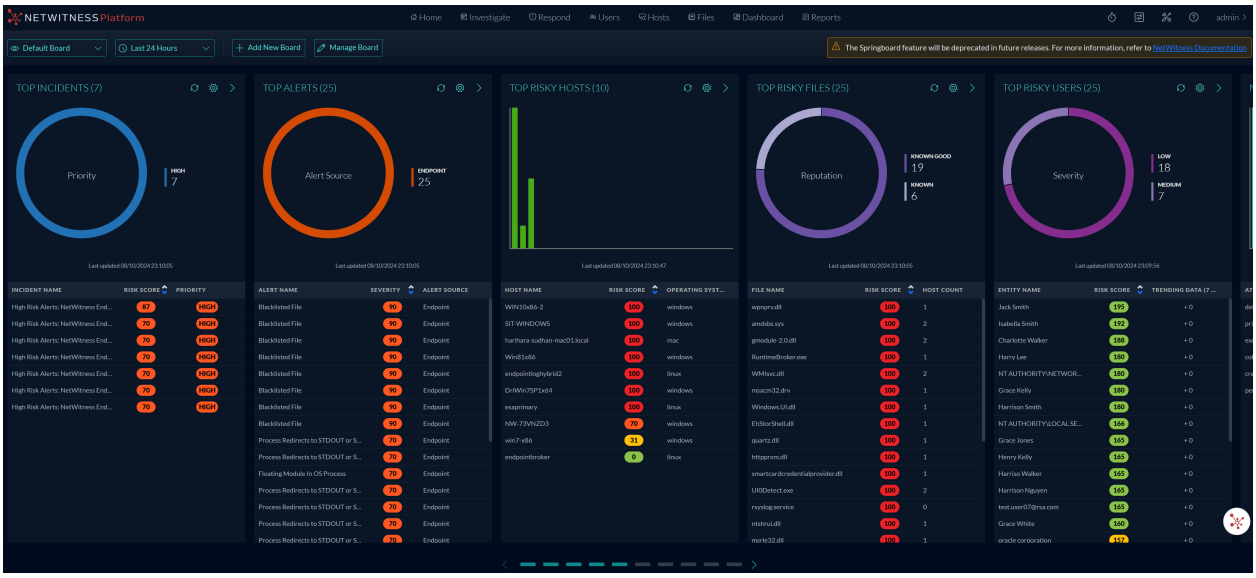
Note: From NetWitness 12.5 and later, the **Home** page will be the default landing page for users installing the NetWitness Platform for the first time. For existing users, Springboard will still be the default landing page. However, the Springboard feature will be deprecated in future releases, and the Home page will become the default landing page. Users can click the **Home Page** to view the new widgets.

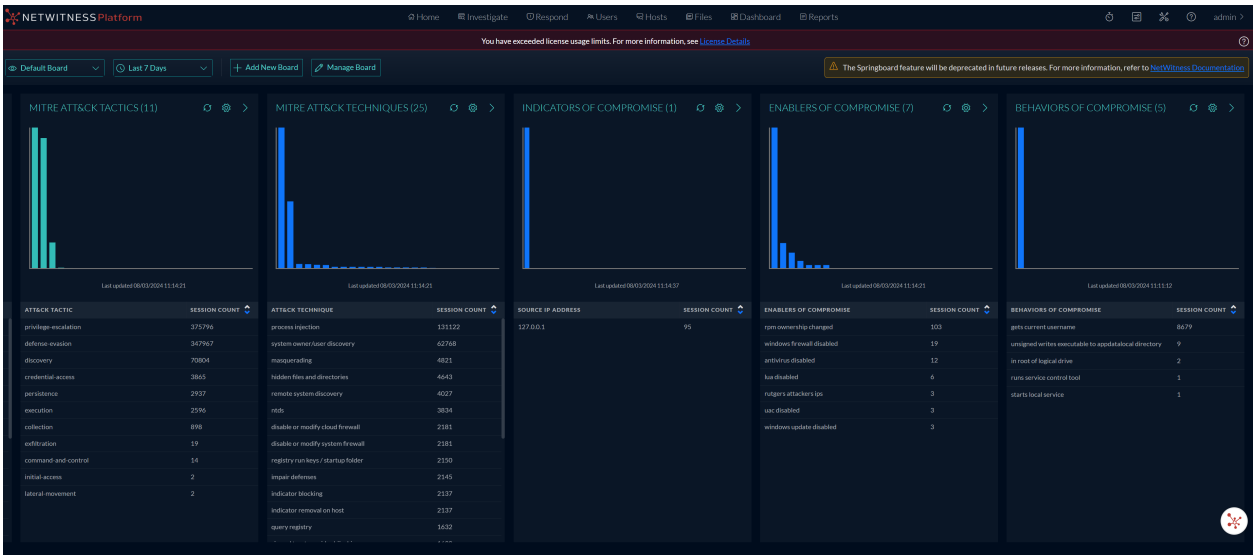
What can I do here?	Path	Show me how
View out-of-the-box widgets Customize the widget layout • Add widgets • Edit a widget configuration • Delete widgets • Rearrangement and resizing of widgets • Reset the Dashboard Layout to its default view View details of selected widgets	Home view	See Manage Home Widgets.

Springboard

NetWitness Platform Springboard is an easy-to-use landing page that presents platform-wide detections and signals in a single view to help analysts hunt and investigate faster than ever before.

Click the NetWitness logo at the top left corner to view the Springboard if you have the set the landing page as the default landing page.





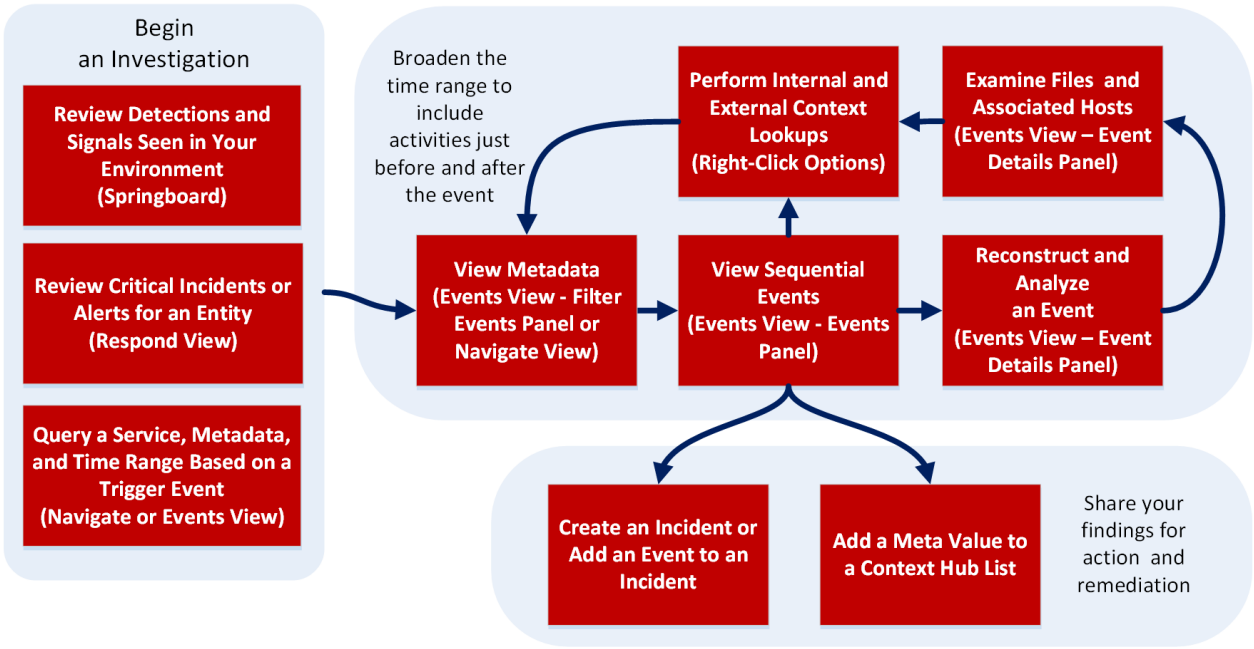
What can I do here?	Path	Show me how
View out-of-the-box panels Edit a panel Add New Board Refresh a panel Select time range View all incidents, alerts, users, files, and hosts View details of selected incident, alert, user, file, and host Manage Board (add, rearrange, and delete panels) Add a new custom private board	Springboard view	See Managing the Springboard.

Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

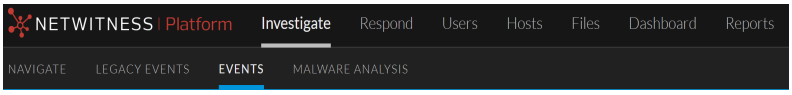
Investigate

The Investigate view is the tool for SIEM, network, and endpoint data investigation, presenting different views into a set of data. Analysts can see metadata and raw data for endpoints, logs, and events, as well as potential indicators of compromise. In addition to investigating data on a specific service, you can pivot into Investigate from Respond, the Dashboard view, an entry in a report generated by the Reporting Engine, or a properly configured third-party application.

You can begin your investigation in any Investigate view, then continue the investigation seamlessly in another Investigate view. The manner in which you proceed is determined by the question that needs to be answered. If you find an event that needs a response, you can create an incident in Respond where an incident responder will take further action. The following figure depicts the high-level flow of an investigation. The *NetWitness Investigate User Guide* provides detailed information.



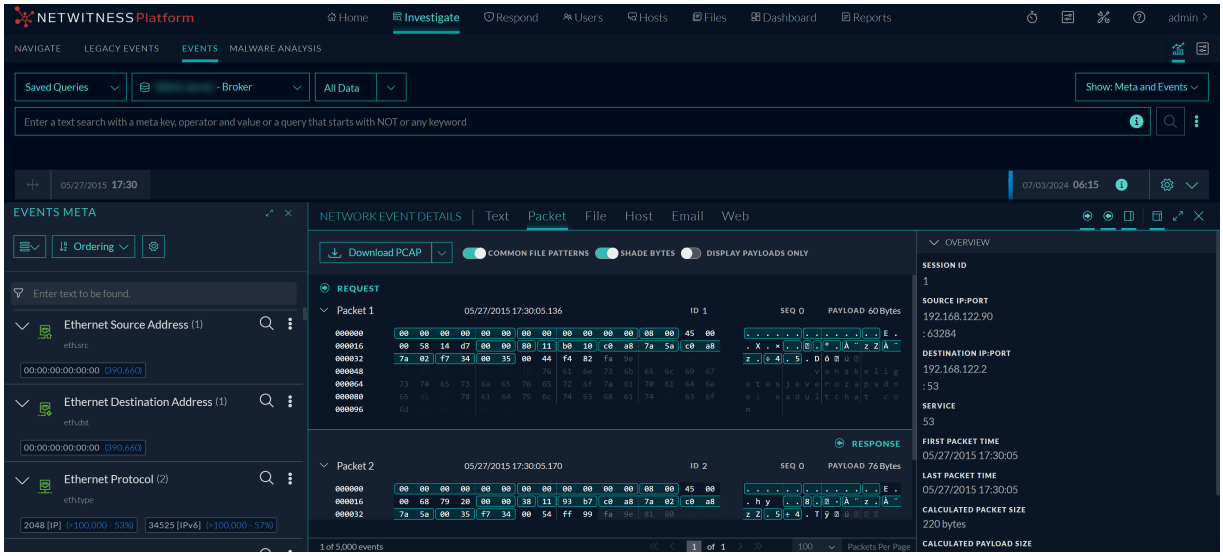
Investigate Menu



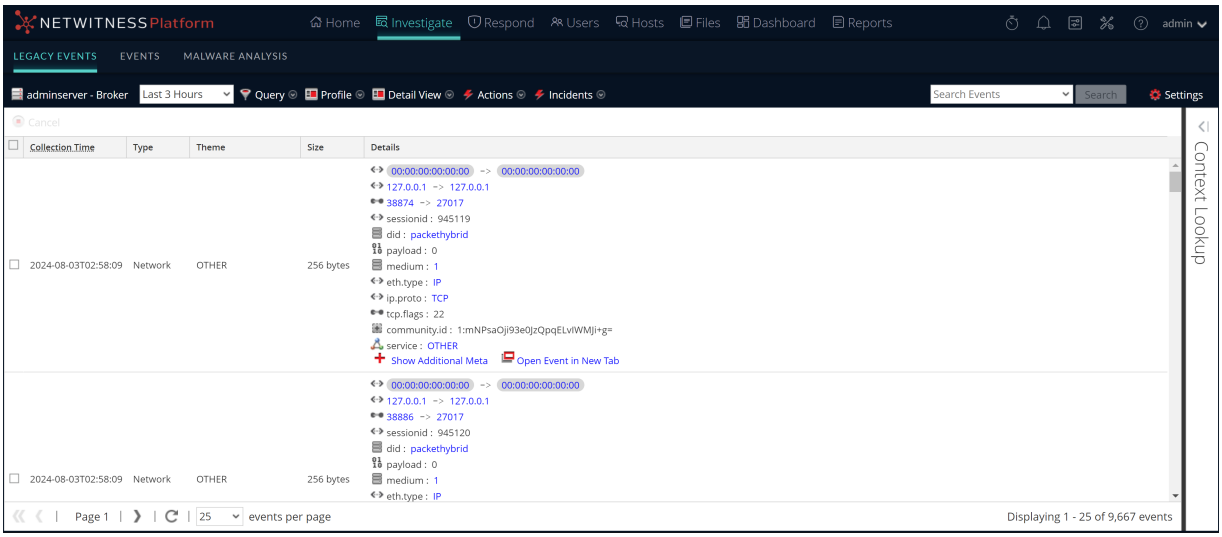
The Investigate menu has the following options:

- **Navigate**: The Navigate view provides a list of meta keys and meta values with a focus on metadata. You can drill into the data, search for events, open a selected event in the Events view, and look up additional context from the Context Hub service.

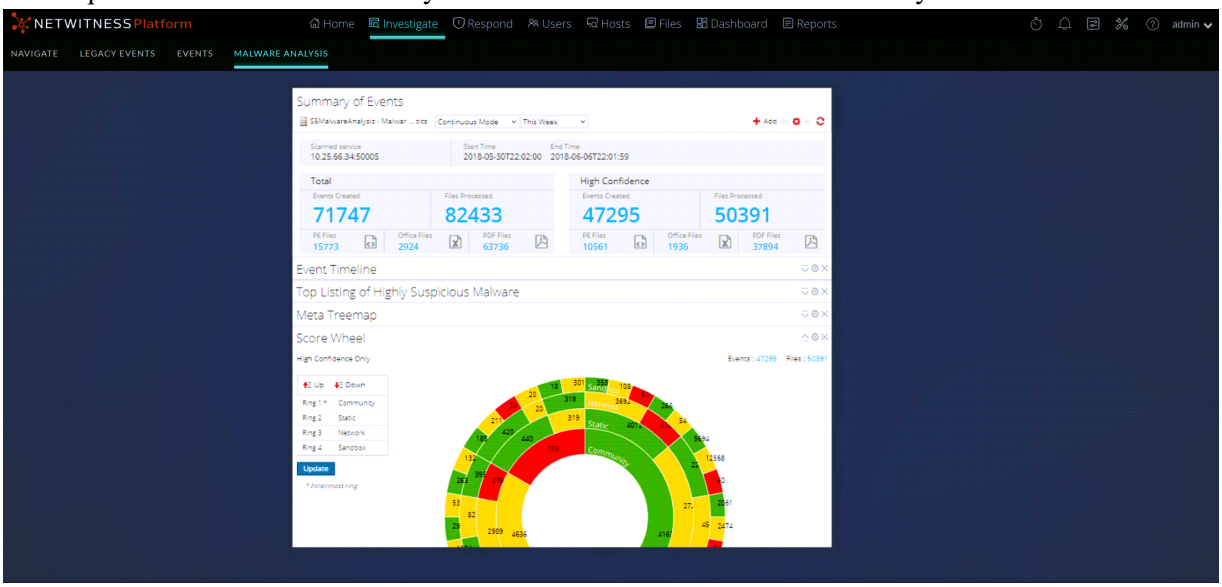
- **Events**: The Events view (formerly Event Analysis view) is the default user interface for interacting with events. It provides a sortable list of events with focus on metadata and raw data. You can search for events, view a reconstruction that offers helpful cues to identify points of interest, pivot to standalone Endpoint, look up additional context from the Context Hub service, look up data in Live, do external lookups, and create an incident for incident responders. By default only the Events view appears in the menu, but when the Legacy Events view is enabled, both the Events view and the Legacy Events view are visible in the menu bar.



- **Legacy Events**: With major functionality added to the Events view, the Legacy Events is no longer needed and it is hidden unless the administrator enables it. The Legacy Events view provides a list of events with a focus on raw data. You can browse a simple list of events, a detailed list, and a log list. You can search for events, view a reconstruction of an event, look up additional context from the Context Hub service, and create an incident for incident responders.



- **Malware Analysis**: Malware Analysis is an automated malware analysis processor designed to analyze certain types of file objects (for example, Windows PE, PDF, and MS Office) to assess the likelihood that a file is malicious. Using Malware Analysis, you can prioritize the massive number of files captured in order to focus analysis efforts on the files that are most likely to be malicious.



What can I do here?	Path	Show me how
Configure Investigate Views and Preferences	Investigate view	See "Configuring Investigate Views and Preferences" in the *NetWitness Investigate User Guide*.

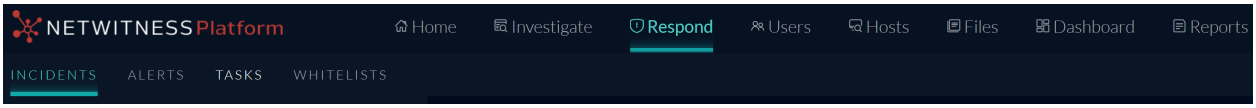
What can I do here?	Path	Show me how
Browse Event Metadata	Navigate view	See "Refining the Results Set" in the *NetWitness Investigate User Guide*.
Browse Raw Events	Events view	See "Refining the Results Set" in the *NetWitness Investigate User Guide*.
Analyze Raw Events and Metadata	Events view	See "Reconstructing and Analyzing Events" in the *NetWitness Investigate User Guide*.
Scan Files and Events for Malware	Malware Analysis view	See the *Malware Analysis User Guide*.
Triage an Incident	Pivot from the Respond view	See the *NetWitness Respond User Guide*.

Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Respond

The Respond view presents analysts with a queue of incidents in severity order. When you take an incident from the queue, you receive relevant supporting data to help you investigate the incident. From there, you can determine the incident scope and escalate or remediate it as appropriate.

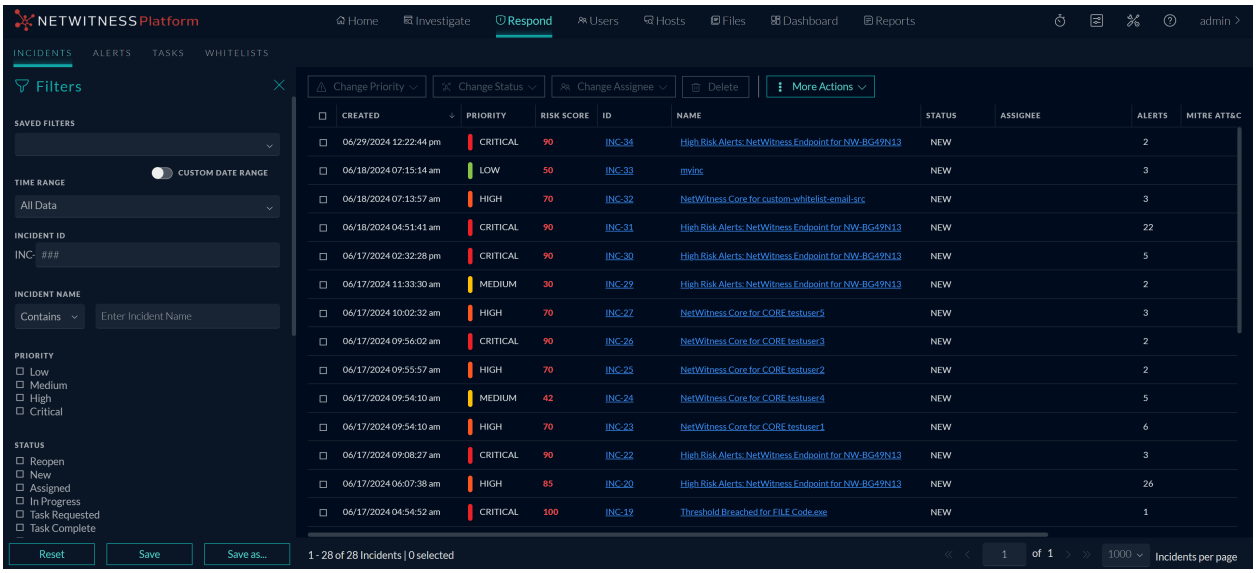
Respond Menu



The Respond menu has the following options:

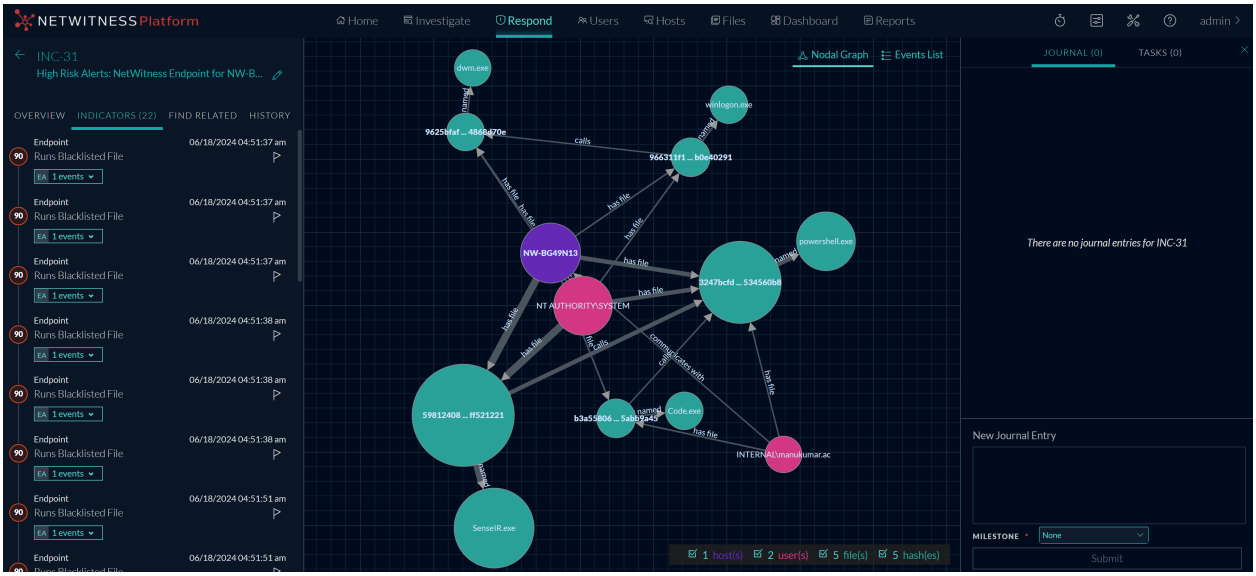
- **Incidents**: The Incidents List view contains a list of all incidents with basic information. The Incident Details view provides extensive details about the incident.
- **Alerts**: The Alerts List and Alert Details views provide information about all of the threat alerts and indicators received by NetWitness in one location.
- **Tasks**: The Tasks List view enables you to create tasks and track them to completion.
- **Whitelists**: The Whitelists view enables you to whitelist the unwanted and recurring non-suspicious alerts for sources such as Endpoint, Insight, ESA and NetWitness Core.

The following figure shows the Respond view - Incidents List view, which shows a list of prioritized incidents.

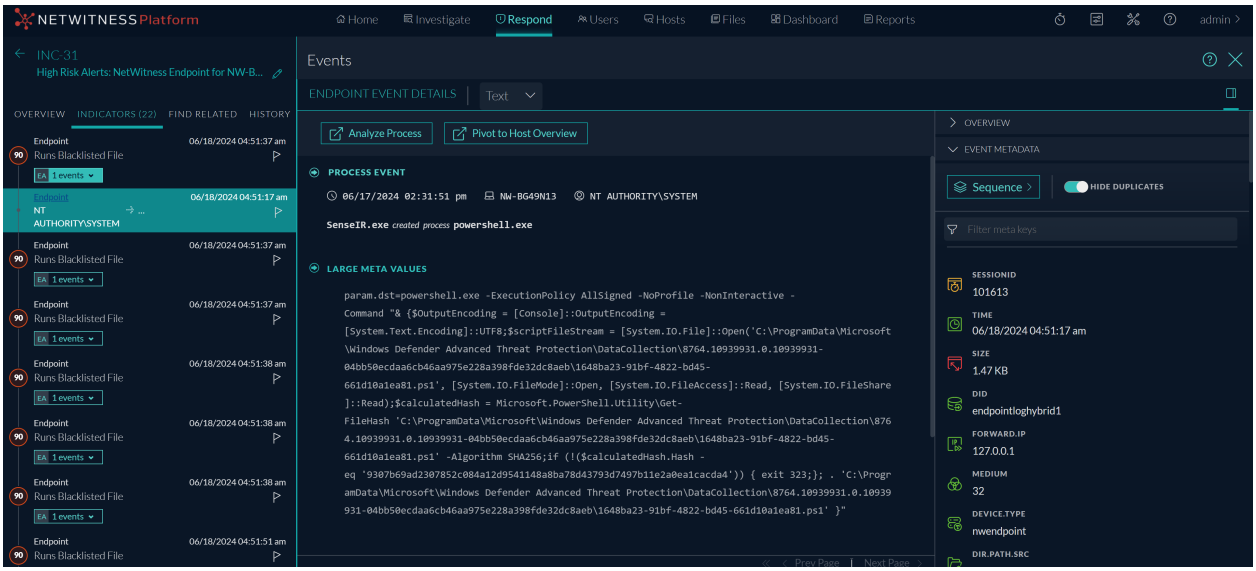


When using NetWitness as your case management tool, you can also manage incidents from this view. New incidents appear at the top of the incident queue.

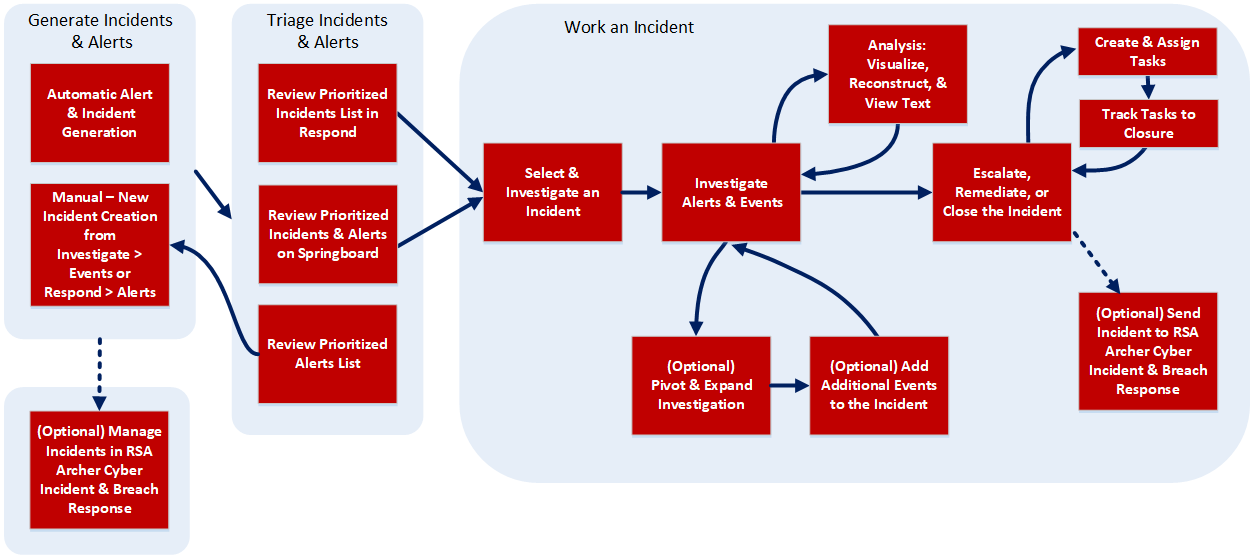
The following figure shows an example of the Respond view - Incident Details view, which shows details for a selected incident.



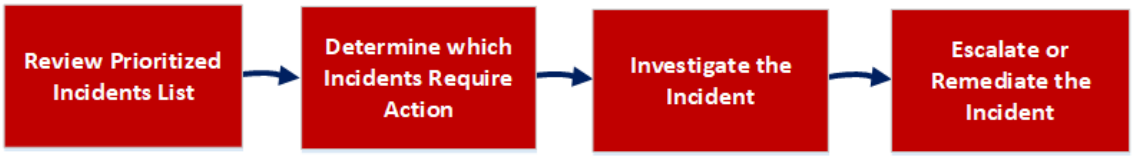
The Respond view is designed to make it easy to evaluate incidents, contextualize that data, collaborate with other analysts, and pivot to a deep-dive investigation as needed. The following figure shows an example of an event analysis in the Incident Details view.



The following figure shows the high-level Respond workflow process.



The following figure shows the high-level process that Incident Responders use to respond to incidents in the Respond view.



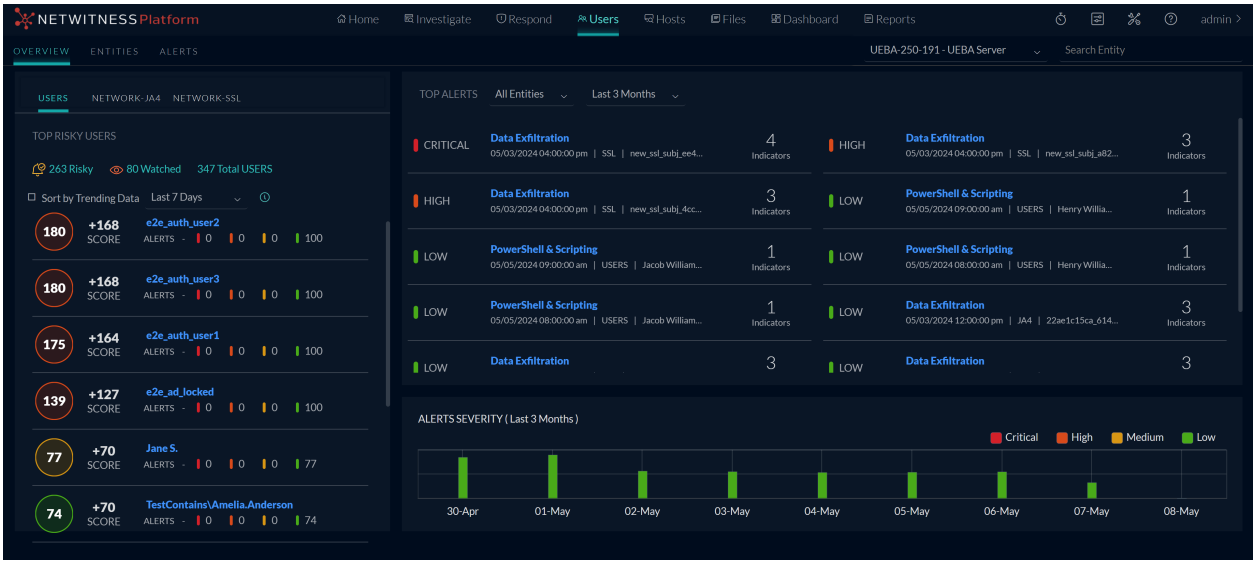
In the Respond view, analysts look at the prioritized list of incidents and determine which incidents require action. They click an incident for a clear picture of the incident with supporting details and they can investigate the incident further. Analysts can then determine how to respond to the threat, by escalating or remediating it.

What can I do here?	Path	Show me how
View prioritized incident lists	Respond > Incidents (Incidents List view)	See the *NetWitness Respond User Guide*.
Determine which incidents require action (Triage an incident)	Respond > Incidents (Incident Details view)	See the *NetWitness Respond User Guide*.
Investigate the incident	Respond > Incidents (Incident Details view)	See the *NetWitness Respond User Guide*. (You can also pivot to the Investigate view.)
Escalate or Remediate the Incident	Respond > Incidents (Incident Details view) and Respond > Tasks (Tasks List view)	See the *NetWitness Respond User Guide*.
Review Alerts	Respond > Alerts (Alerts List and Alert Details views)	See the *NetWitness Respond User Guide*.

Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Users

The Users view provides visibility into risky user behaviors across your enterprise with NetWitness UEBA. You can view a list of high-risk users and a summary of the top alerts for risky behavior for your environment. Then you can select a user or an alert and view details about the risky behavior and a timeline during which the behaviors occurred.



The Users menu has the following options:

- **Overview**: It provides an initial view into the recent and most important user or network entity activities in the environment. Each panel shows either prioritized incidents for investigation or consolidated metrics reflecting potential risks to the enterprise.
- **Entities**: It is a proactive threat hunting console. You can use behavioral filters to build use case driven target lists, and to continuously monitor the environment for specific risky behavior patterns.

Note: The Entities view is only available if you are assigned the role of Administrator or UEBA Analyst.

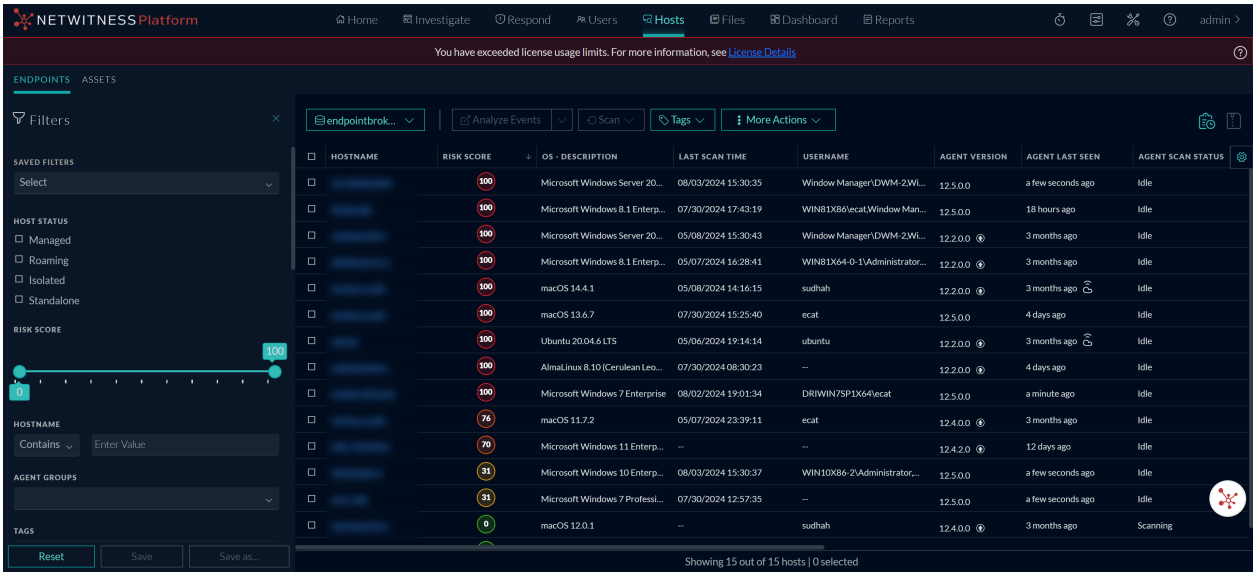
- **Alerts**: It displays details about all the alerts in your environment. You can view forensic information about suspicious activity in your environment that is based on a specific timeframe.

What can I do here?	Path	Show me how
Find Risky User Behavior	Users view	See the *NetWitness UEBA User Guide*.

Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Hosts

The Hosts view lists all hosts that have a NetWitness Endpoint agent running. You can filter hosts based on operating system, agent last seen, last scan time, risk score, and other factors. You can open a specific host to view events related to alerts, anomalies, process details, and information related to logged-in users.

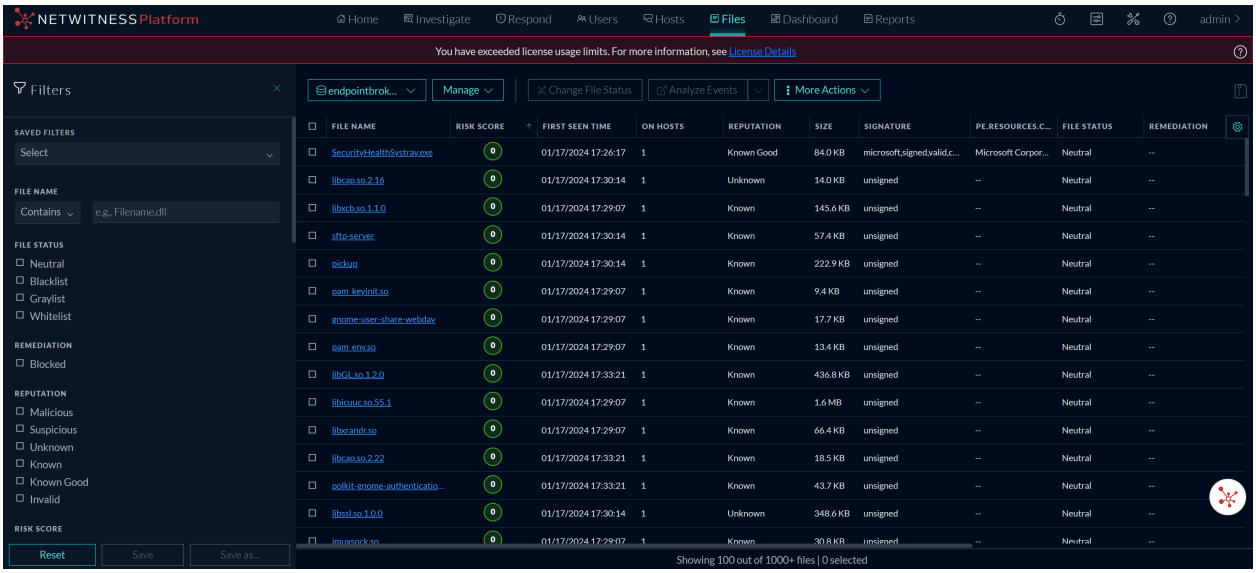


What can I do here?	Path	Show me how
Investigate Endpoints	Hosts view	See the *NetWitness Endpoint User Guide*.

Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Files

The Files view provides a holistic view of all files in your deployment. You can apply filters, sort, and categorize files by status to reduce the number of files for analysis, and identify suspicious or malicious files.

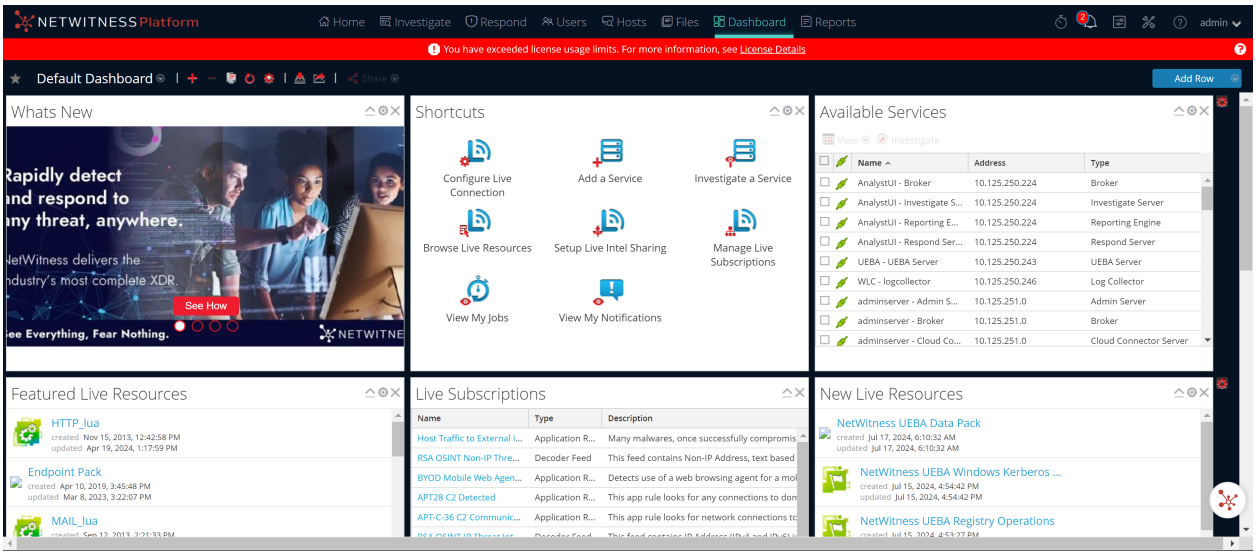


What can I do here?	Path	Show me how
Find Suspicious Endpoint Files	Files view	See the *NetWitness Endpoint User Guide*.

Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Dashboard

A dashboard is a group of dashlets that give you the ability to view data in one space, the key snapshots of the various components that you consider important. In NetWitness® Platform, you can compose dashboards to obtain high-level information and metrics that portray the overall picture of a NetWitness Platform deployment, displaying only the information that is most relevant to the day-to-day operations.



NetWitness Platform has predefined dashboards that you can select in the Dashboard view depending on the tasks you perform:

You can select the following preconfigured dashboards:

- Default
- Identity
- Investigation
- Operations - File Analysis
- Operations - Logs
- Operations - Network
- Operations - Protocol Analysis
- Overview
- RSA SecurID
- Threat - Hunting
- Threat - Intrusion
- Threat - Malware Indicators

What can I do here?	Path	Show me how
Select a Dashboard	Dashboard view	See Managing Dashboards.
Create a Dashboard	Dashboard view	See Managing Dashboards.
Manage Dashboards	Dashboard view	See Managing Dashboards.

Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Reports

The Reports view enables you to view and manage reports relevant to your SOC role according to your assigned permissions.

Reports Menu

The Reports menu has the following options:

- **Manage**: This panel allows you to create or modify an rules, reports, charts, alerts, and lists as per the requirement.
- **View**: You can view a report or list of all reports. You can also view the scheduled reports to know the state of the scheduled report. If the scheduled report is in a stop or disable state, you can start or enable the scheduled report.

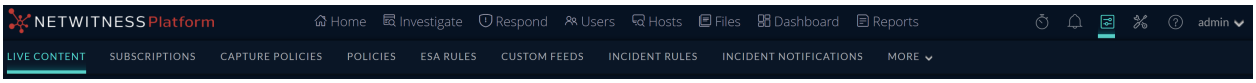
What can I do here?	Path	Show me how
View a Report	Reports > View	See the *Reporting User Guide*.
Manage Reports	Reports > Manage	See the *Reporting User Guide*.

Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Configure

The Configure view enables Threat Intel personnel (Content Experts) to configure data sources and inputs to NetWitness in one convenient location.

Configure Menu



The Configure menu has the following options:

- **Live Content** (Live Services): The Live Content view enables you to search for and subscribe to Live Services resources. Live Services is the component of the NetWitness that manages communication and synchronization between NetWitness services and a library of Live content available to NetWitness customers. You can view, search, deploy, and subscribe to content from the RSA Live Content Management System (CMS) to NetWitness services and software. When you subscribe to a resource, you agree to receive updates on a regular basis from RSA Live Services.

- **Subscriptions** (Live Services): The Subscriptions view enables you manage the Live content that you subscribed to, in the Live Content view. To set up Live Services on NetWitness, you configure the connection and synchronize between the CMS server and NetWitness.
- **Capture Policies**: The Capture Policies view enables you to set up selective network data collection, which gives you the ability to apply centrally managed capture policies across your Network Decoders. This results in better use of service resources, including hard drive space, which leads to more predictable costs and lessens the burden of managing multiple services. You can determine which traffic is stored and how it is stored by using policies. Each policy contains a list of supported base protocols and definitions for handling any other protocols that are detected.
- **Policies**: The Policies view contains two sub-tabs, namely **Configuration** and **Content**.
  - **Configuration**: Centralized Service Configuration via policy allows you to manage the configuration of services in your environment efficiently. The Decoder, Concentrator, and Log Decoder deployed in your environment may be large in number and geographically distributed.
  - **Content**: Policy-based Centralized Content Management enables you to find, deploy, and manage content through the entire life cycle based on policies that can be assigned to groups of devices. It is a single location to view, modify and manage the content deployed across all services in the environment.
- **Incident Rules**: The Incident Rules view enables you to create incident rules with various criteria to automatically create incidents. You can view prioritized incidents in the Respond view.
- **Incident Notifications**: The Incident Notifications view enables you to automatically send email notifications to SOC Managers and the Analysts assigned to the incidents when incidents are created or updated.
- **ESA Rules**: The ESA Rules view enables you to manage the Event Stream Analysis (ESA) rules that specify criteria for problematic behavior or threatening events in your network. When ESA detects a threat that matches the rule criteria, it generates an alert.
  You can create ESA rules yourself or download them from Live Services. The Rule Library shows all ESA rules created or downloaded. To activate rules, you have to add them to a deployment. Deployments map rules from your rule library to the appropriate ESA services.
- **Custom Feeds** (Live Services): The Custom Feeds view streamlines the task of creating and managing custom feeds, as well as populating the feeds to selected Decoders and Log Decoders. You can set up and maintain custom and identity feeds.
  NetWitness uses feeds to create metadata based on externally defined metadata values. A feed is a list of data that is compared to sessions as they are captured or processed. For each match, additional metadata is created.
  You can create custom feeds to provide extra metadata extraction, for example, to accommodate custom network applications.
- **Log Parser Rules**: The Log Parser Rules tab displays information about individual log parsers, as well as the default, "parse all" parser that can parse logs that are not associated with a particular log parser. This tab contains the following information:

- You can view the rules for a particular event source type, including the default parser.
- You can view the names, literals, patterns, and metadata for each configured log parser.
- You can add log parsers.
- You can add, edit, and delete custom rules for log parsers.

- **Service Topology**: The Service Topology tab enables administrators and analysts to view all the NetWitness core services in a hierarchical layout depicting the collection and aggregation of the services in your deployment. This visualization displays the topology for Broker, Concentrator, Log Decoder, Packet Decoder, Hybrids, ESA and Log Collector.

What can I do here?	Path	Show me how
Create a Live Services account.	RSA Live Registration Portal: https://cms.netwitness.com/registration/	See the *Live Services Management Guide*.
Find and deploy Live Services resources.	(Configure) > Live Content	See the *Live Services Management Guide*.
Set up selective network data collection.	(Configure) > Capture Policies	See the *Decoder Configuration Guide*.
Set up Live Services Services on NetWitness.	(Configure) > Subscriptions	See the *Live Services Management Guide*.
Create Policies and Groups.	(Configure) > Policies	See the *Host and Services Getting Started Guide*.
Create Policies and Groups.	(Configure) > Policies	See the *Live Services Management Guide*.
Create incidents automatically.	(Configure) > Incident Rules	See the *NetWitness Respond Configuration Guide*.
Configure incident notifications.	(Configure) > Incident Notifications	See the *NetWitness Respond Configuration Guide*.
Configure alerts.	(Configure) > ESA Rules	See the *Alerting with ESA Correlation Rules User Guide*.
Set up and maintain custom and identity feeds.	(Configure) > Custom Feeds	See the *Live Services Management Guide*.
View and edit log parsers and log parser rules.	(Configure) > Log Parser Rules	See the *Log Parser Customization Guide*.
View Topology for different core services	(Configure) > Service Topology	See the *Host and Services Getting Started Guide*.

Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Admin

In the Admin view, administrators can manage network hosts and services; monitor the health and wellness of NetWitness; and manage system-level security. They can also configure global system resources and manage event sources.

Admin Menu

The (Admin) menu has the following options:

- **Hosts**: The Hosts view is where you set up and maintain hosts. A host is the machine on which services run and a host can be a physical or virtual machine.
- **Services**: The Services view enables you to manage services, manage service users and roles, maintain service configuration files, and explore and edit service properties. A service performs a unique function, such as a Decoder service, which captures network data in packet form.
- **Event Sources**: The Event Sources view enables you to manage event sources and configure alerting policies for them. Organizations typically monitor event sources in groups based on the criticality of the event sources. You can create monitoring policies for each event source group and order them based on priority.
- **Endpoint Sources**: The Endpoint Sources view enables you to manage and update endpoint agent configurations through groups and manage the agents behavior using policies. You can either use the default policies or customize these policies.
- **Health & Wellness**: The Health & Wellness view enables you to monitor the health of the NetWitness hosts and services in your network environment.
- **System**: The System view enables you to set global NetWitness configurations. You can configure global audit logging, email, system logging, jobs, RSA Live Services, URL integration, Investigation, Event Stream Analysis (ESA), ESA Analytics, and advanced performance settings. In addition, you can manage NetWitness versions and configure the local licensing server.
- **Security**: The Admin Security view provides the capability to manage user accounts, manage user roles, map external groups to NetWitness roles, and modify other security-related system parameters. These apply to the NetWitness system and are used in conjunction with the security settings for individual services.

What can I do here?	Path	Show me how
Manage hosts.	(Admin) > Hosts	See the *Host and Services Getting Started Guide*.

What can I do here?	Path	Show me how
Manage services including managing service user access and security.	(Admin) > Services	See the *Host and Services Getting Started Guide*.
Manage event sources and configure alerting policies for them.	(Admin) > Event Sources	See the *Event Source Management Guide*.
Manage endpoint sources and configure alerting policies for them.	(Admin) > Endpoint Sources	See the *Event Source Management Guide*.
Set up and monitor alarms for the hosts and services in your NetWitness domain.	(Admin) > Health & Wellness > Alarm	See the *System Maintenance Guide*.
Monitor statistics for the NetWitness hosts and the services running on the hosts.	(Admin) > Health & Wellness > Monitoring	See the *System Maintenance Guide*.
Create and apply policies to your hosts and services to help you maintain the health and wellness of your NetWitness domain.	(Admin) > Health & Wellness > Policies	See the *System Maintenance Guide*.
Set global configurations for NetWitness.	(Admin) > System	See the *System Configuration Guide*.
Configure Global Audit Logging.	(Admin) > System > Global Auditing	See the *System Configuration Guide*.
Set up system security.	(Admin) > Security	See the *System Security and User Management Guide*.
Manage system users with roles and permissions.	(Admin) > Security	See the *System Security and User Management Guide*.
Set up Public Key Infrastructure (PKI) authentication. PKI is available in NetWitness.	(Admin) > Security	See the *System Security and User Management Guide*.

Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Setting Up Your Default View by SOC Role

After logging in to NetWitness, you can navigate into the application easier by setting up your default view based on your Security Operations (SOC) role. You can set your default view, also known as a landing page, in your user preferences.

On upgrade to version 12.5 or later, by default the **Home** page is displayed if you have not configured the default landing page in previous versions.

In previous versions, if you configured the default landing page as Respond or Investigate in the User Preferences, then on upgrade to version 12.5, the default landing page will be Respond or Investigate view.

On fresh install of NetWitness 12.5 version, when you log in, by default **Home** is the landing page.

The following figure shows the main NetWitness views.

- **Home**: This view is for Admin, Analyst and SOC Manager. Each home page is comprised of multiple widgets. Administrators, Analysts, and SOC Managers can access the respective widgets that display certain data in graphical form. The data can be associated with Endpoints, Users, Assets, Content, Incidents, Alerts, MITRE ATT&CK, Retention, and many more.
- **Springboard**: This view is for Analysts, who can see panels for prioritized alerts, incidents, risky hosts, risky users, risky files, and focused event data to help hunt and investigate faster than ever before.
- **Investigate**: This view is for Threat Hunters, who investigate and hunt for advanced threats. Other analysts such as Incident Responders may pivot into this view for deeper analysis of an incident.
- **Respond**: This view is for Incident Responders, who can view a list of incidents to triage and alerts.
- **Users**: This view is for SOC Managers and Analysts to discover, investigate, and monitor risky behaviors across entities namely Users and Network in your environment.
- **Hosts**: This view is for Analysts, who can investigate or perform analysis on hosts using attributes such as IP address, host name, Mac address, risk score, and so on.
- **Files**: This view is for Analysts, who can investigate or perform analysis on files using attributes such as IP address, host name, Mac address, risk score, and so on.
- **Dashboard**: This view is for all users. You can view dashboards on different areas of interest depending on your user permissions. You have the option to select a preconfigured dashboard, import a dashboard, or create your own custom dashboard.
- **Reports**: This view is for all users. You can view reports on different areas of interest depending on your user permissions.
-  **Configure**: This view is for Threat Intel personnel (Content Experts), who configure data sources and inputs to NetWitness. Content Experts use this area to download and manage Live content. They can also create and manage incident and ESA rules.

-  **Admin**: This view is for System Administrators, who set up and maintain the overall application.

You can select any of the main NetWitness views as your default view. In addition to the main views, NetWitness has predefined dashboards that you can select in the Dashboards view depending on the tasks you perform:

- Default Dashboard
- Identity Dashboard
- Operations - Logs Dashboard
- Operations - Network Dashboard
- Overview Dashboard
- Threat - Indicators Dashboard
- Threat - Intrusion Dashboard

The following table shows typical SOC roles and the available views you can select as your landing page in your user preferences based on your SOC role. If you have more than one role, select the view that is most appropriate for you to start with when you log in to NetWitness.

SOC Roles	Role Description	Consider this Default Landing Page
Incident Responder (Tier 1 Analyst)	Addresses incidents and alerts queued for them to review and mitigate.	**Springboard** or **Respond**
Threat Hunter (Tier 2/Tier 3 Analyst)	Investigates and hunts for advanced threats.	**Springboard**, **Investigate**, **Users**, **Hosts**, or **Files** For information on selecting the default Investigate view, see the *NetWitness Investigate User Guide*.
SOC Manager (SOC Management and Reporting)	Manages SOC readiness and responds to incidents and data breaches.	**Springboard** or **Dashboard** When you log in, select the appropriate predefined dashboard for your SOC role. You can also import a dashboard or create your own dashboard.
Content Expert (Threat Intelligence)	Configures data sources and inputs to NetWitness.	**Dashboard** or  (Configure) When you log in, select the appropriate predefined dashboard for your SOC role. You can also import a dashboard or create your own dashboard. If you choose Dashboard as your default view, you can navigate to the  (Configure) view from the main menu.

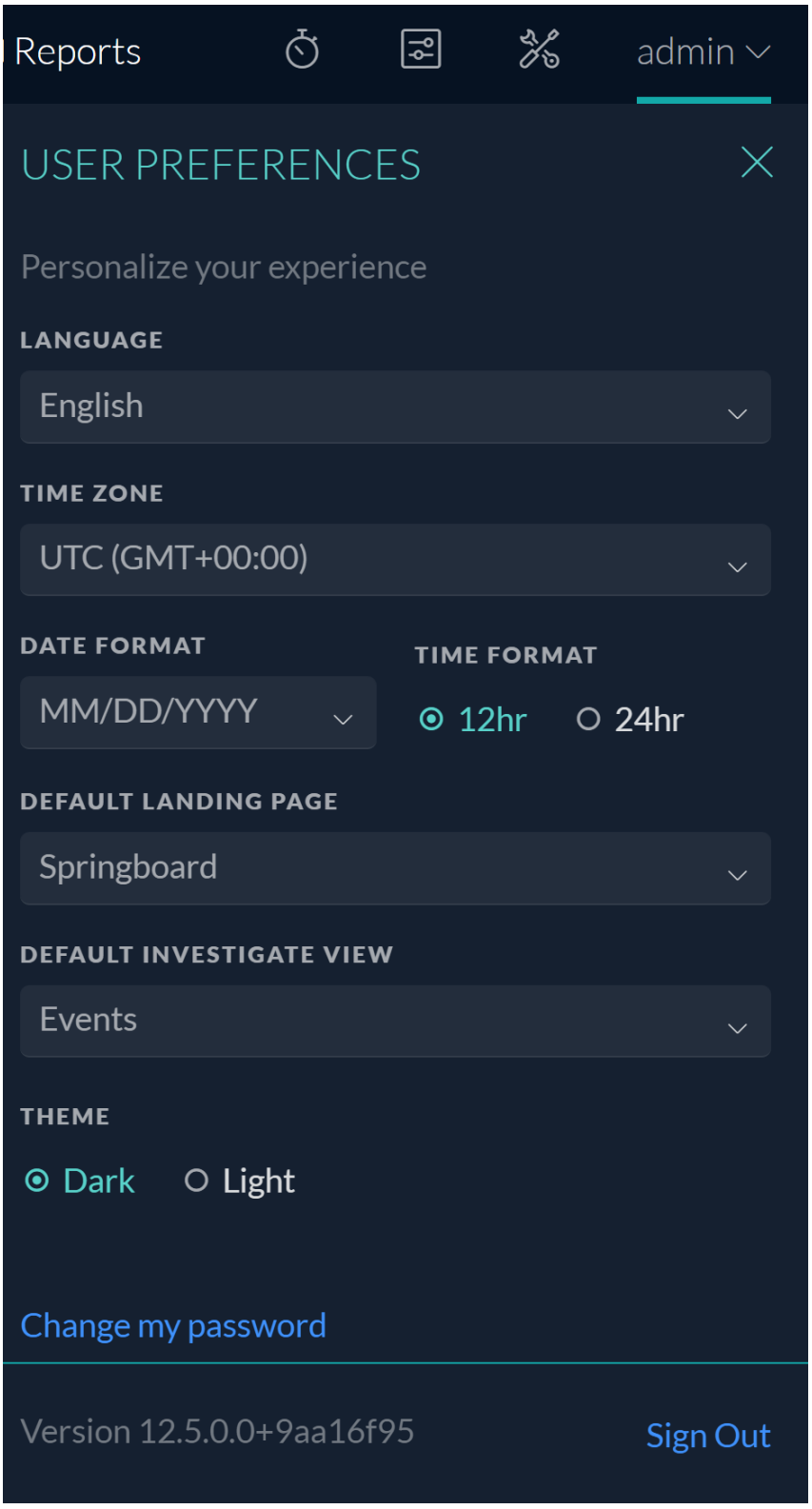
SOC Roles	Role Description	Consider this Default Landing Page
Data Privacy Officer (DPO)	Similar to an Administrator, but a DPO monitors and protects privacy-sensitive information.	**Dashboard** When you log in, select the appropriate predefined dashboard for your SOC role. You can also import a dashboard or create your own dashboard.
System Administrator	Focuses on the configuration and stability of the overall application. Manages user access.	**Springboard**

Set Your Default View

1. On the main menu bar, select your username, for example, 

.

   The User Preferences dialog shows your current preferences.


Reports
admin
USER PREFERENCES
Personalize your experience
LANGUAGE
English
TIME ZONE
UTC (GMT+00:00)
DATE FORMAT
MM/DD/YYYY
TIME FORMAT
12hr
24hr
DEFAULT LANDING PAGE
Springboard
DEFAULT INVESTIGATE VIEW
Events
THEME
Dark
Light
Change my password
Version 12.5.0.0+9aa16f95
Sign Out

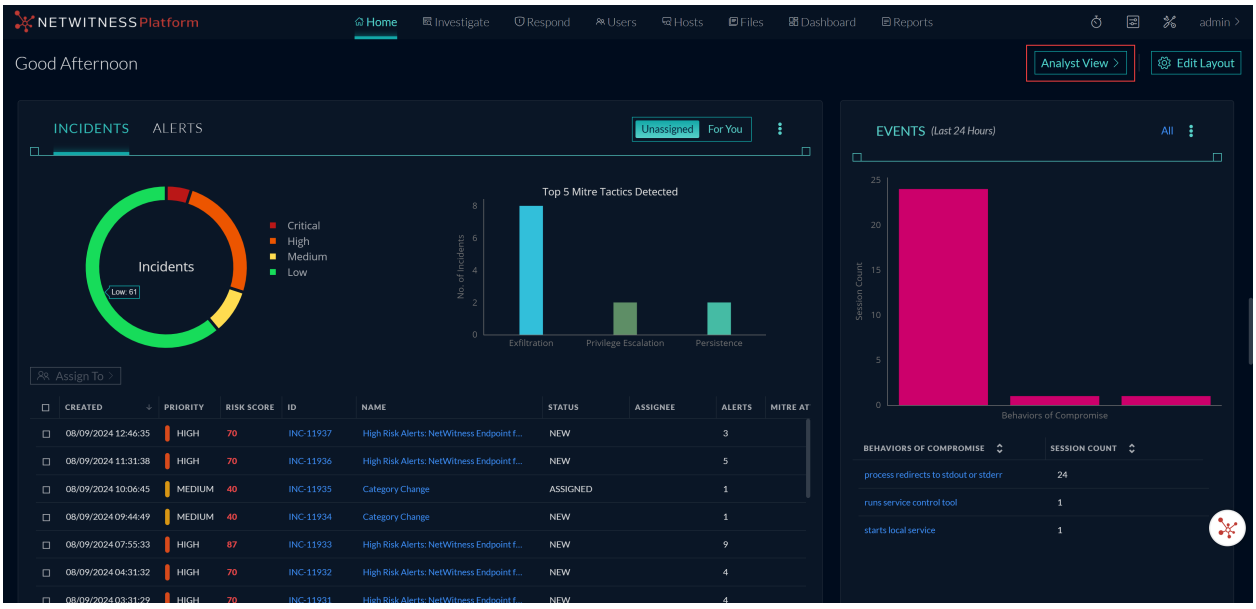
2. In the **Default Landing Page** field, select the default view that you would like to see when you log in to NetWitness. Use the above table to make your selection based on your SOC role. For example, if you are an Analyst, you can select **Springboard**; if you are an Incident Responder you can select **Respond**; and if you are a Threat Hunter, you can select **Investigate**.

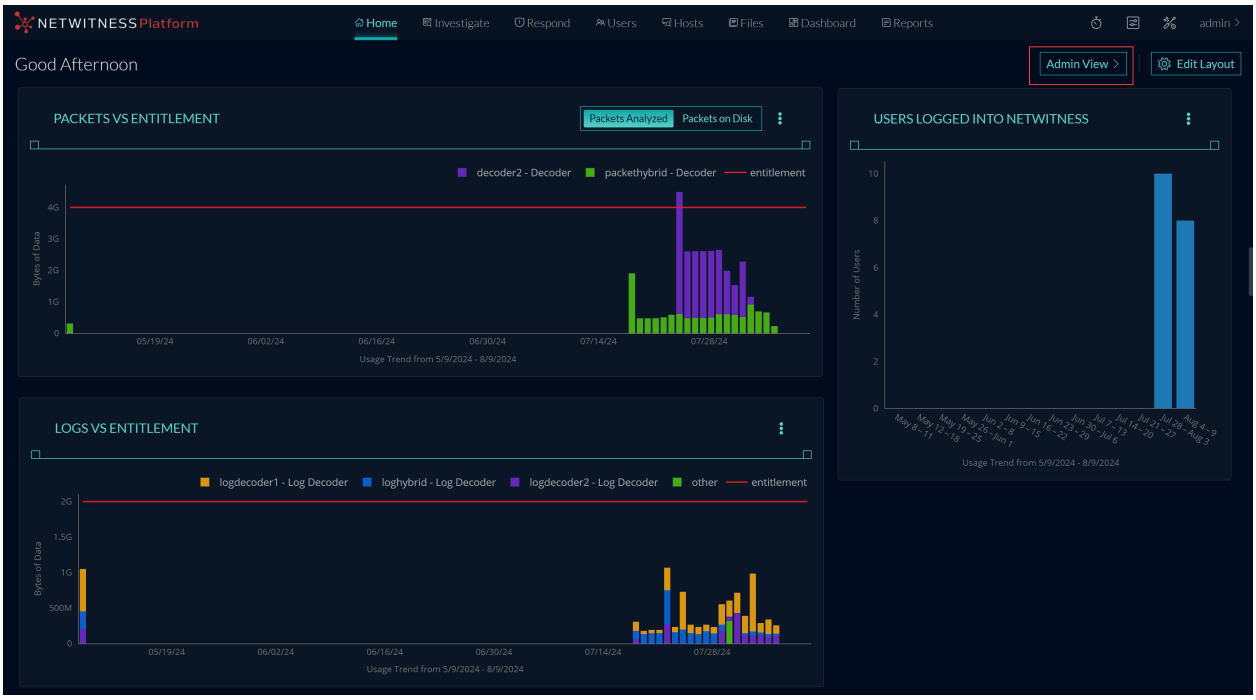
   Your preferences become effective immediately. You can change your default landing page at any time. For information on other preferences, see Setting User Preferences.

3. To verify that you can see the correct default view, click **Sign Out** to log out and then log back in to NetWitness.

Manage Home Widgets

(From 12.5 and later) NetWitness introduces a new **Home** page menu that consists of **Admin**, **Analyst**, and **Manager** views. Each home page is comprised of multiple widgets. Administrators, Analysts, and SOC Managers can access the respective widgets that display certain data in graphical form. The data can be associated with Endpoints, Users, Assets, Content, Incidents, Alerts, MITRE ATT&CK, Retention, and many more.





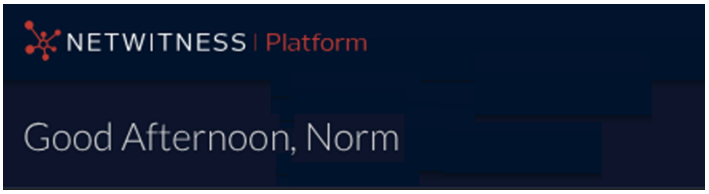
Access Home Page

Log into the NetWitness platform and click the **Home** page.

From NetWitness 12.5 and later, the **Home** page will be the default landing page for users installing the NetWitness Platform for the first time and the you can click the **Home Page** to view the new widgets from the Admin, Analyst, and Manager views.

On the default home page, in the top left corner, a greeting to the user is displayed. If available, the user's name is shown following the greeting.

For example: **Good Afternoon, Norm**



If the username is not available, then only the greeting will be displayed.

Note: The full name of a NetWitness user is displayed. NetWitness will only display the name of users created within it. Users who have been created through Single Sign-On, Active Directory, or any other type of user will not have their names displayed.

Customize the Dashboard Layout

The widgets for the Home page are arranged in a predefined layout for the various roles (analyst, manager, and admin). These layouts can be customized to suit your individual needs. Altering the layout of a dashboard is restricted to the Edit Layout mode, which is activated by clicking the Edit Layout button on the upper right of the screen.

The following actions can be performed while in Edit Layout mode:

- Addition of widgets to the dashboard.
- Deletion of widgets from the dashboard.
- Rearrangement and resizing of widgets to achieve a desired layout.
- Reset the Dashboard Layout to its default view.

Add a Widget

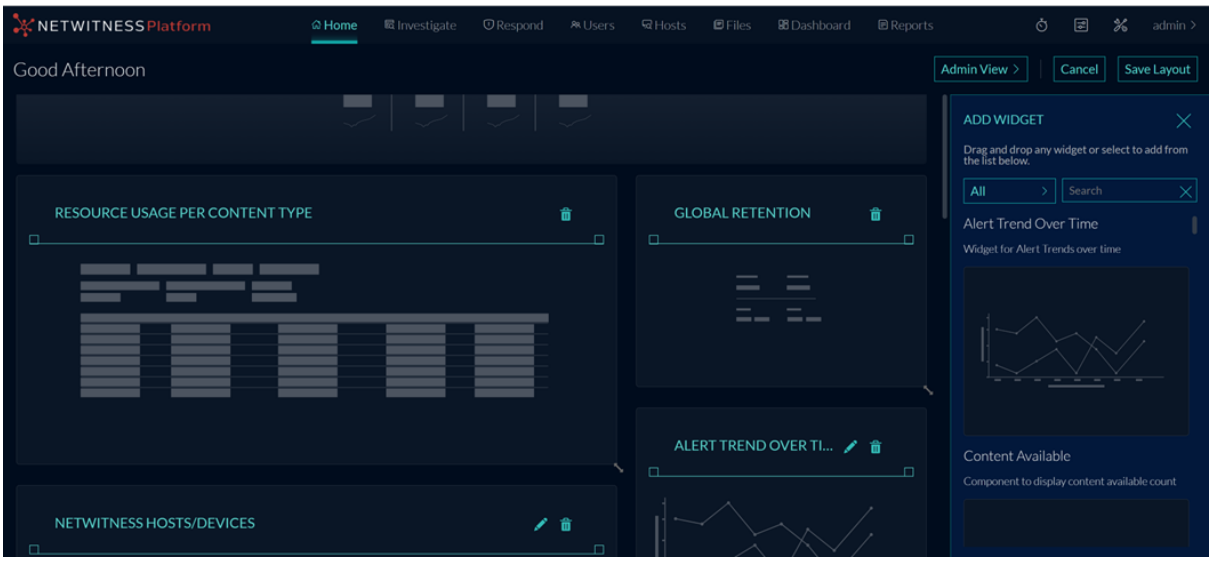
Users have the liberty to add widgets to their dashboard. There is no restriction on the number of widgets that can be added.

To add a widget to the dashboard

1. Log in to the NetWitness Platform and navigate to the **Home** page.
2. From the drop-down menu in the upper right-hand corner of the Home page, users should select the view they want to modify (**Admin**, **Analyst**, or **Manager**).
3. Click the **Edit Layout** button in the upper right corner. The **Add Widget** panel displays all the widgets that are available.

   Note:
   • To quickly locate a widget, use the Search field by entering its name. The widgets will be filtered as the user types, displaying only matching results.

• Click the **X** icon in the upper right corner to close the Add Widget panel.

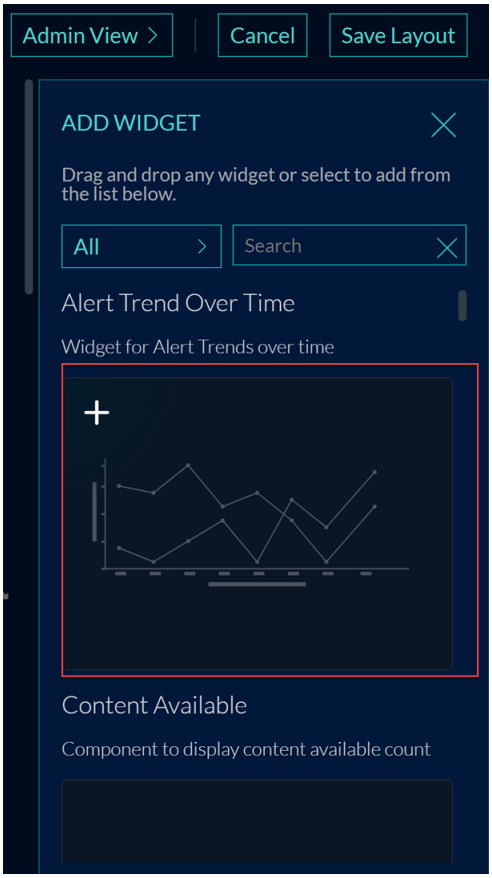


4. To add a widget, follow either of the steps below:

   a. Hover the cursor over the desired widget, triggering a + (add) icon to appear in its upper-left corner. Click on the + icon to add the widget. This will add the widget to the bottom of the layout.

   b. Alternatively, click and drag a widget to the desired location on the dashboard. As the user drags

the widget, the dashboard will indicate the target position.



5. To save the changes to the dashboard layout, click **Save Layout**.

   When the user clicks the Cancel button, any unsaved changes made to their dashboard layout are discarded, and the panel is closed.

   Note: Modifications to a layout are applicable only to the user who made them.

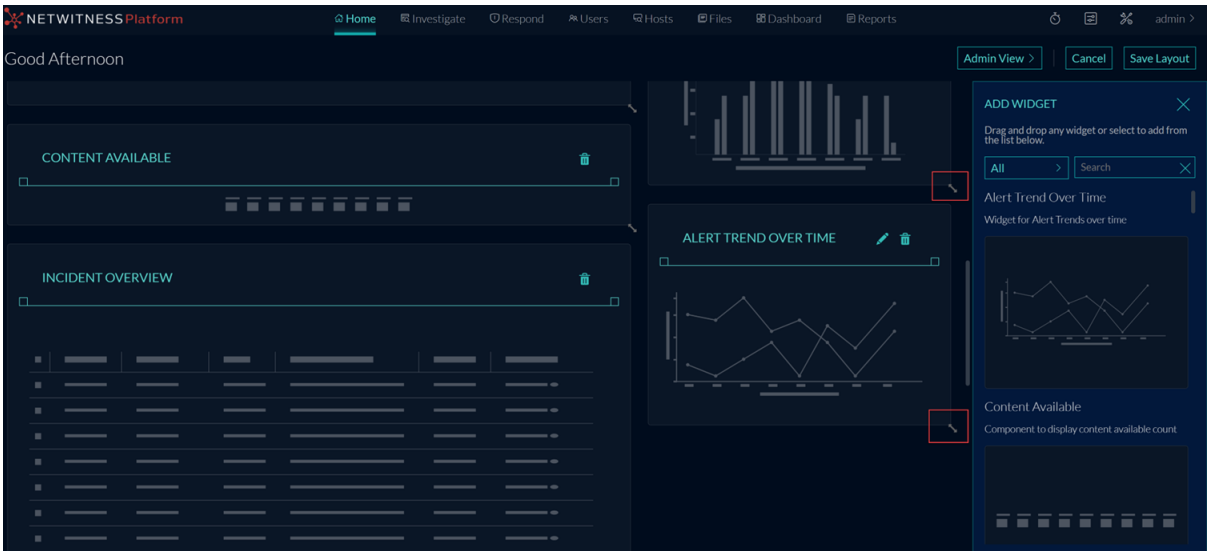
Rearrange and Resize Widgets

Users have the flexibility to adjust the dashboard layout according to their preferences. Widgets can be resized and rearranged to emphasize content deemed critical.

Note: The **MITRE ATT&CK Overview** and **Overview** widgets have a fixed position and size on the dashboard and thus cannot be rearranged or resized.

- To rearrange a widget, simply select and drag it to the desired location within the layout. Adjacent widgets will adjust automatically to accommodate the change.
- For resizing, an arrow appears at the bottom right corner of all widgets upon hover. Click and drag it to adjust the dimensions. Horizontal dragging alters width, vertical dragging modifies height, and diagonal dragging adjusts both dimensions proportionally

Note: Each widget possesses default dimensions that can be modified within certain limits. Minimum and maximum size constraints are enforced.



Delete Widgets

Users can delete one or more widgets. However, users can only delete widgets for which they have the required permissions.

To delete a widget from the dashboard

1. Click the Delete icon  located at the upper right corner of the widget. A confirmation message will appear.

2. Click **Delete** to permanently remove the widget from the dashboard. The remaining widgets will be adjusted to fill the vacated space if possible.

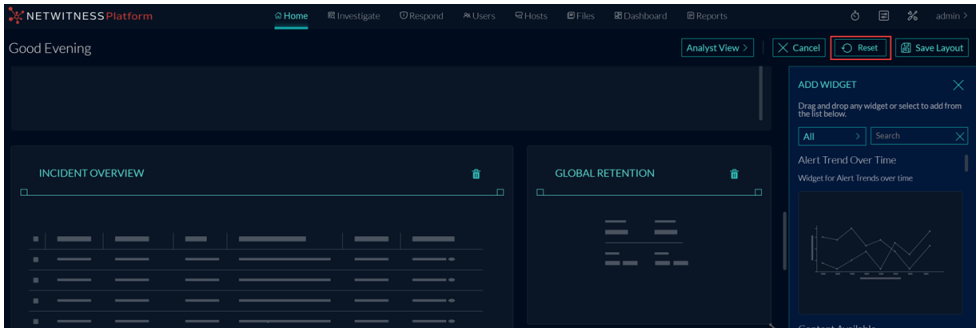
Reset the Dashboard Layout

Users can reset the dashboard to clear any dashboard customizations and restore the dashboard to the current default configuration.

To Reset the Dashboard Layout

1. Click the **Edit Layout** button in the upper right corner and click **Reset**. A confirmation message will appear.

   Note: Resetting the dashboard will remove any customizations users have made and revert the dashboard layout to its default view.



2. Click **Reset**. The page refreshes and reverts to the default view.

Admin View

The Admin dashboard offers a comprehensive overview of the system's status and health using widgets including information about resource usage, retention, content, incident trends, and licensing utilization. The Admin dashboard view consists of several out-of-the-box widgets as follows:

- Overview
- What's New Widget
- Resource Usage per Content Type
- Logs vs Entitlement
- Packets vs Entitlement
- NetWitness Hosts/Devices
- Users Logged into NetWitness
- Global Retention
- Content Available

- Mean Time to Detect (MTTD)
- Mean Time to Resolve (MTTR)
- Alert Trend Over Time
- False Positives (Incidents)
- Incident Overview

Overview

This Overview widget is displayed as the top most widget in the Admin view and it consists of the following 5 cards.

- **Mean Time to Detect**: This card displays the mean time to detect incidents in Respond.
- **Mean Time to Resolve**: This card displays the mean time to resolve incidents in Respond.
- **Incidents**: This card displays the total number of incidents created in the last 24 hours.
- **New Incidents**: This card displays the total number of incidents which are still in the New state for the last 24 hours.
- **Closed Incidents**: This card displays the total number of incidents which are closed in the last 24 hours.

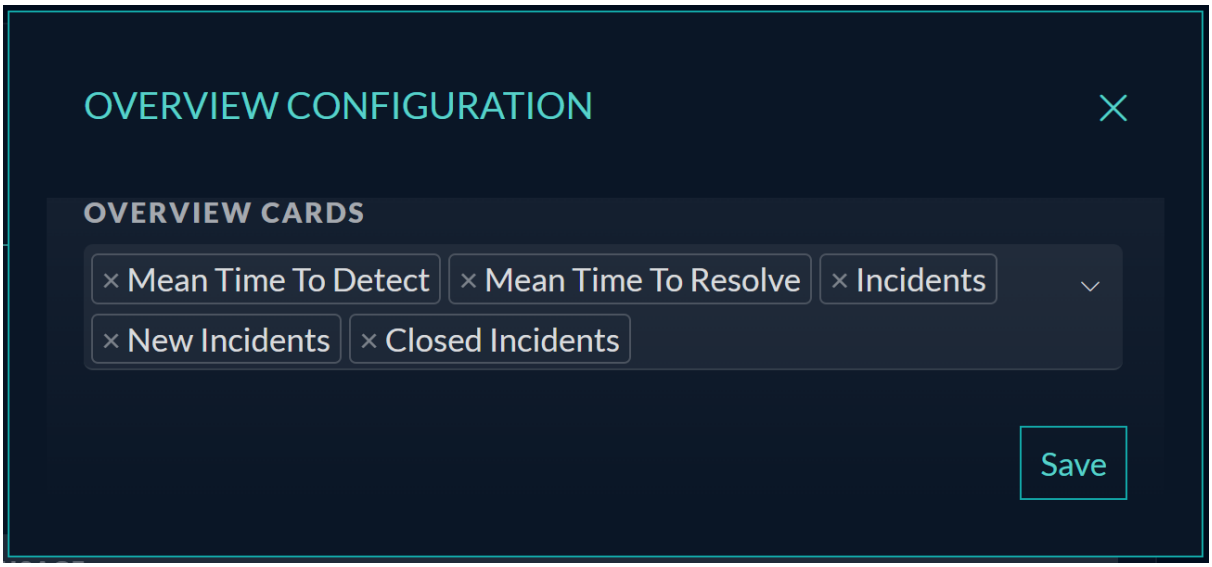
By default, this widget displays the last 24 hours data when you log in to the NetWitness Platform.

You can edit the **Overview** widget at any time and add additional cards. However, you can have a maximum of 5 cards displayed at once.

To edit the Overview Widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.

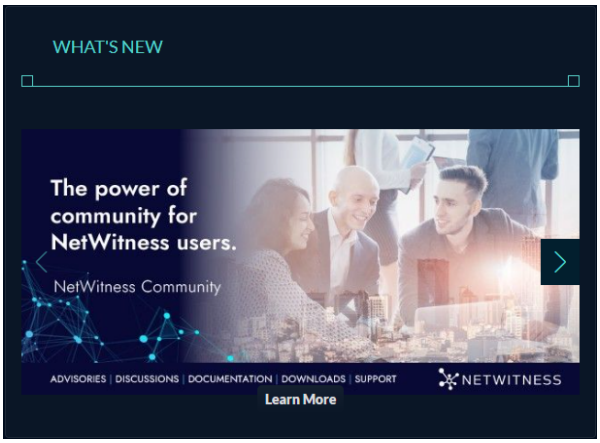
   The **Overview Configuration** dialog is displayed.

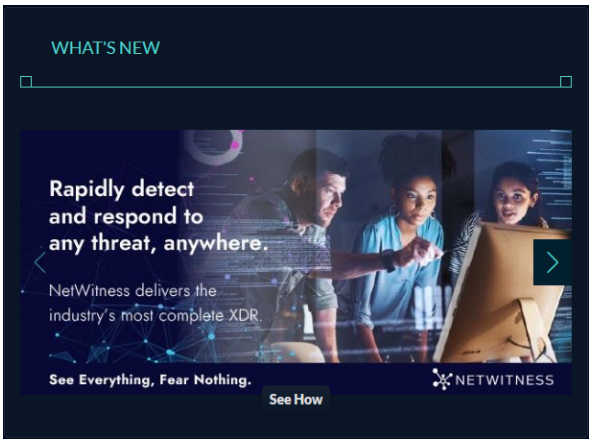


2. Select the required cards from the **Overview Cards** drop-down menu.
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

What's New Widget

NetWitness 12.5.1 introduces the What's New widget, which displays key snapshots of updated and new NetWitness content, blogs, and messages highlighting campaigns, threats, content life cycle updates, and more. The widget provides a centralized platform for conveniently accessing and navigating through all critical data from a single location.

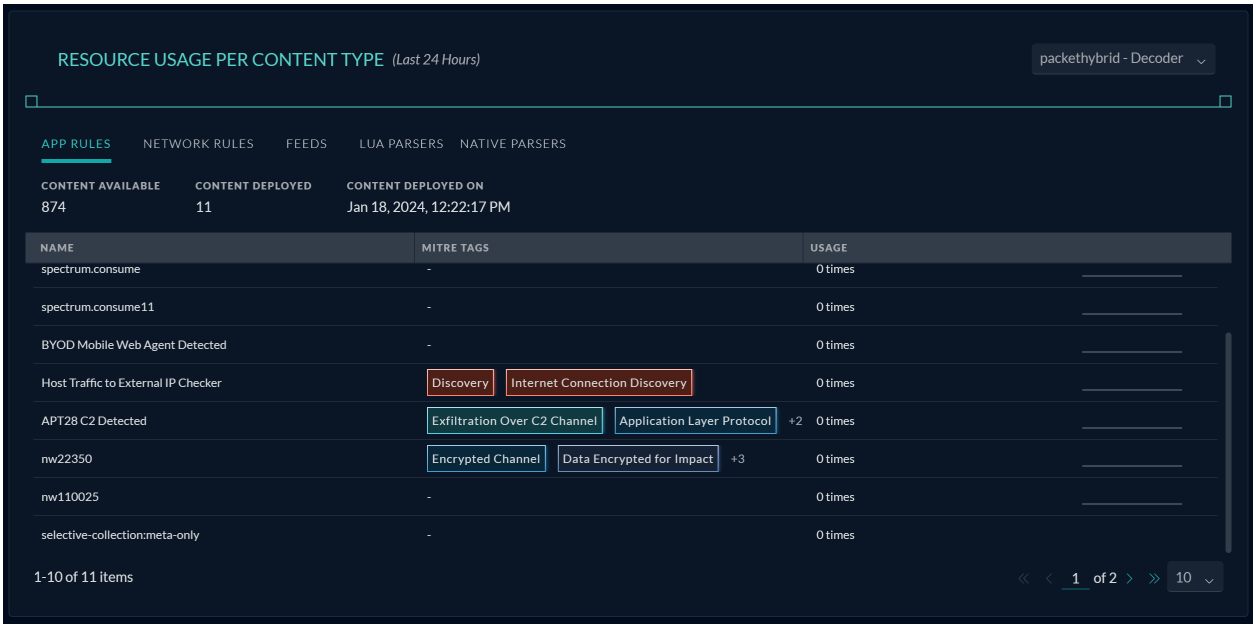




Note: This widget is available by default only in Admin view.

Resource Usage per Content Type

This widget shows various content deployed on the selected decoder, including the memory and usage details. It enables analysts to make informed decisions based on the available decoders' content details. In this widget, content details are available for multiple decoders. Users can switch between multiple decoders by clicking the drop-down on the upper right. For a single host, the host drop-down option is disabled, and the available host is displayed. By default, the last 24 hours of data is displayed.



Note: This widget is available by default only in **Admin** view.

Note:
To allow other users role to view widget metrics, an administrator must grant specific permissions on both the source server and core services.
• Source Server Permissions Required:
- **source-server.contentstats.read**
- **source-server.policy.read**
- **source-server.policy.manage**

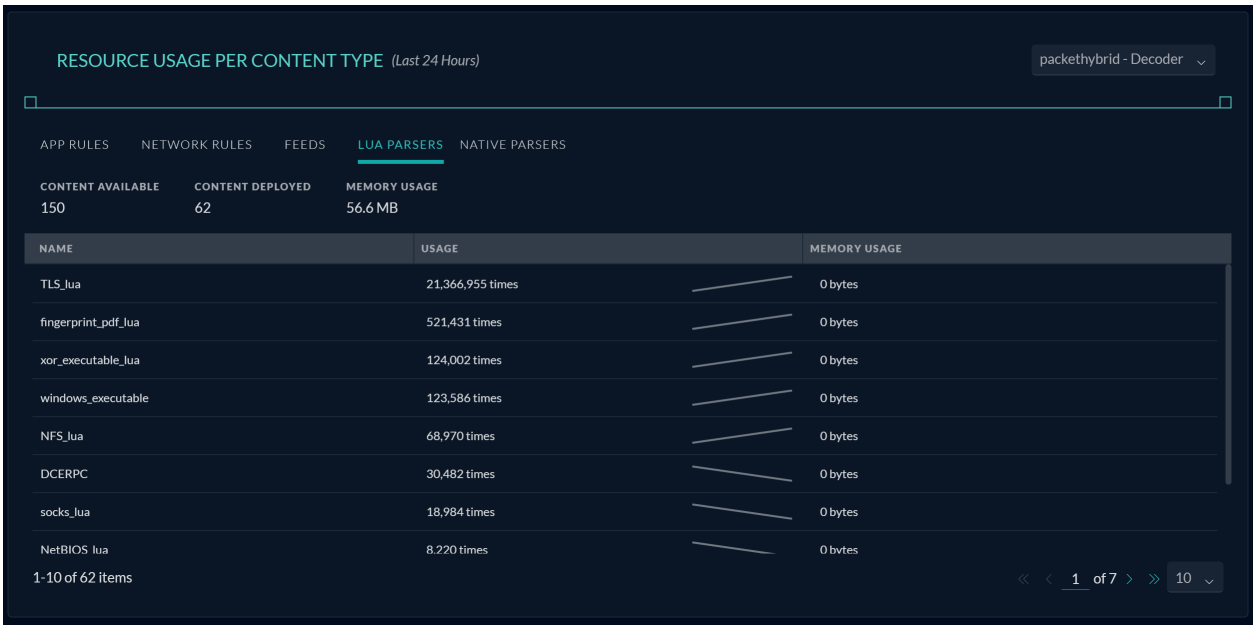
For more information, see the Source-server section in the "Role Permissions" topic in the *System Security and User Management Guide*.
• Core Services Permissions Required:
For each core service (Log Decoders and Packet Decoders) deployed in the environment, the administrator must add the following permissions to the other user's role. However, if the required user role is not available, you need to create a new user role and then assign the necessary permissions.
- **parsers.manage**
- **rules.manage**

For more information, on adding the user role to the service and assigning permission, see the Add a User Role to a Service section in the "Hosts and Services Maintenance Procedures" topic in the *Hosts and Services Getting Started Guide.*

The content types are App Rules, Network Rules, Feeds, Lua Parsers, and Native Parsers. Under the content type, the content available in Live, the content deployed to the services, the content's timestamp (date and time), memory usage, and feed usage are displayed. Also, a table below the content type shows the content name, bundle, miter tag, usage, and memory usage related to the content.

Note: The statistics displayed vary based on the content type selected. Also, if the content deployed is 0, then the content is not available on Live.

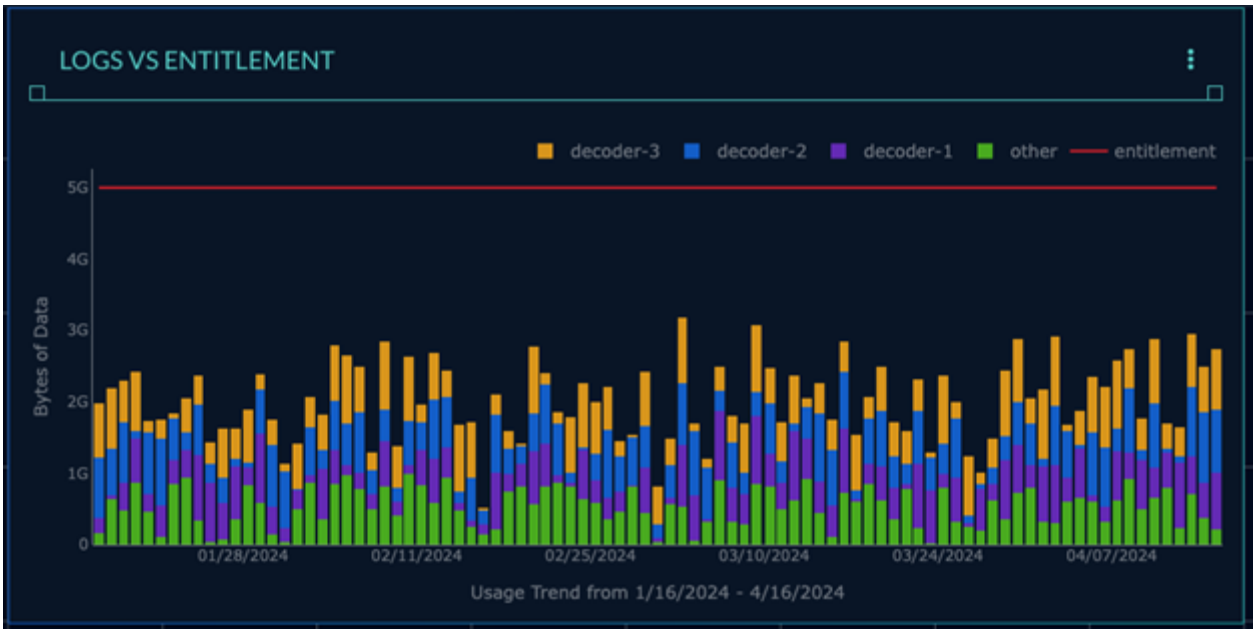
The widget information is paginated. On the bottom right, click the < > or << >> pagination icons to navigate and view the data for other available content.



Logs vs Entitlement

This widget assists system administrators in tracking the volume of log data processed, facilitating a comparison with the allocated licensing quota. It enables administrators to make informed decisions regarding adjustments to their licensing levels, whether to increase or decrease them as necessary.

Note:
• This widget is available by default in **Admin** and **Manager** views.
• To allow other users to view the widget metrics, an administrator must enable **license-server.license.read** permission on the license server. For more information, see the License-server section in the "Role Permissions" topic in the *System Security and User Management Guide*.
• Ensure that the License Server is active to display data on the widget.



A stacked bar graph visually presents the dataset. By default, it showcases the values for the top 5 Decoders processing the highest volume of data. However, users have the option to configure the widget to display data for up to 10 Decoders. Each bar segment in the chart is color-coded to represent a specific Decoder, as indicated by the chart legend. The bar segments are arranged such that the Decoder processing the largest amount of data occupies the top position, followed by others in descending order. The lowest segment represents the aggregated data of all Decoders beyond the configured limit.

Note: The bottom segment may be larger than the other if there are many decoders in the environment.

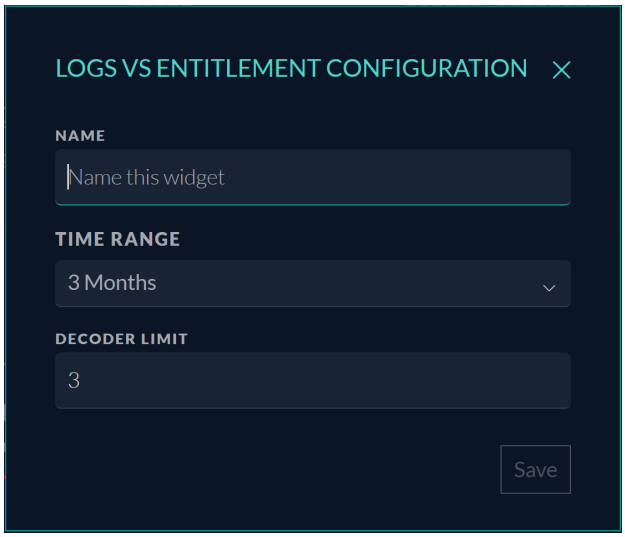
The vertical axis delineates the quantity of data processed, while the horizontal axis displays the dates within the designated time range. Placing the cursor over a graph bar will display a tooltip allowing the user to view the exact values for each Decoder represented. The entitlement line indicates the volume of Log data permitted for processing based on the licensing quota.

Users can edit the existing widget at any time to change its name, time range, or decoder limit, allowing them to customize it according to their preferences.

To edit the Logs vs Entitlement widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.

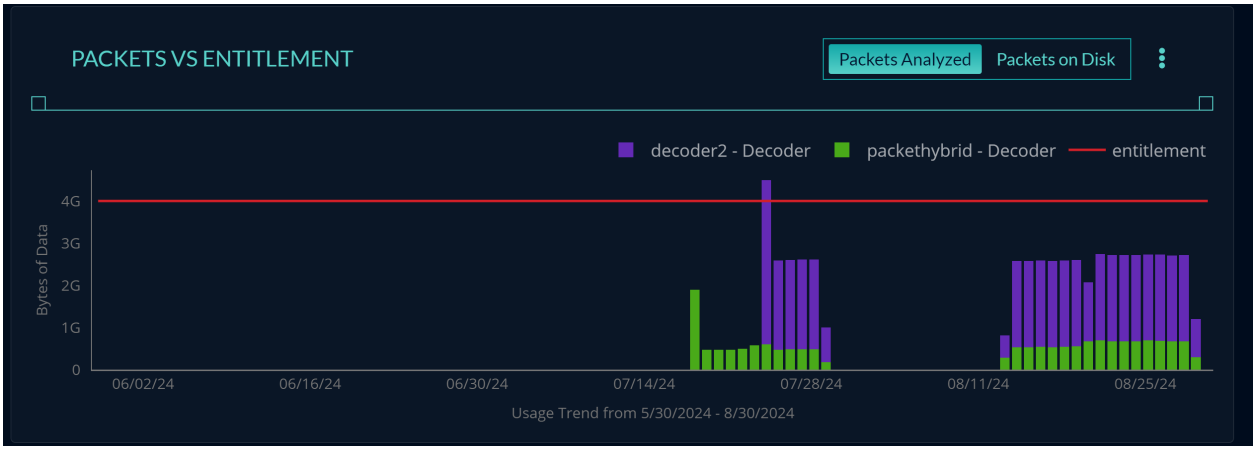
   The **Logs vs Entitlement Configuration** dialog is displayed.



2. Configure the following options based on your preference:
   - **Name**: Enter a desired name for the widget. The name can include alphabets, numbers, spaces, and special characters, such as _ - ( ) [ ].
   - **Time Range**: Select a specific timeframe from the drop-down menu to display data for that period. Available ranges are **3 Months**, **6 Months**, and **9 Months**. By default, 3 months of data are displayed.
   - **Decoder Limit**: Specify the number of decoders to be displayed in the chart. Users can configure a range from 1 to 10 Decoders.
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

Packets vs Entitlement

This widget assists system administrators in tracking the volume of packets processed and packets on disk, facilitating comparison with the allocated licensing quota. It enables administrators to make informed decisions regarding adjustments to their licensing levels, whether to increase or decrease them as necessary. An analysis can be performed based on the volume of packets analyzed, or the physical storage requirements of the packets on disk.



Note:
• This widget is available by default in **Admin** and **Manager** views.
• To allow other users to view the widget metrics, an administrator must enable **license-server.license.read** permission on the license server. For more information, see the License-server section in the "Role Permissions" topic in the *System Security and User Management Guide*.
• Ensure that the License Server is active to display data on the widget.

A stacked bar graph visually presents the dataset. By default, it showcases the values for the top 5 Decoders processing the highest volume of data. However, users have the option to configure the widget to display data for up to 10 Decoders. Each bar segment in the chart is color-coded to represent a specific Decoder, as indicated by the chart legend. The bar segments are arranged such that the Decoder processing the largest amount of data occupies the top position, followed by others in descending order. The lowest segment represents the aggregated data of all Decoders beyond the configured limit.

Note: The bottom segment may be larger than the other if there are many decoders in the environment.

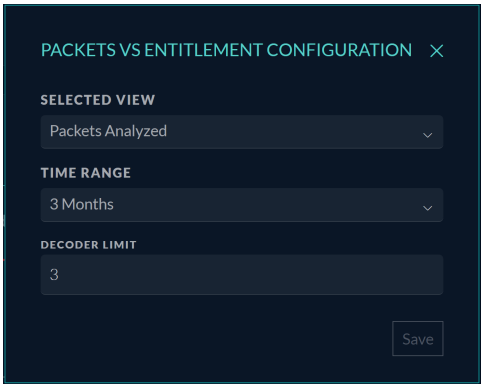
The vertical axis delineates the quantity of data processed or the physical storage used, while the horizontal axis displays the dates within the designated time range. Placing the cursor over a graph bar will display a tooltip allowing the user to view the exact values for each Decoder represented. The entitlement line indicates the volume of Packet data permitted for processing based on the licensing quota.

Users can edit the existing widget at any time to change its view, time range, or decoder limit, allowing them to customize it according to their preferences.

To edit the Packets vs Entitlement widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.

   The **Packets vs Entitlement Configuration** dialog is displayed.



2. Configure the following options based on your preference:
   - **Selected View**: Select either **Packets Analyzed** or **Packets on Disk** option from the drop-down menu.
   - **Time Range**: Select a specific timeframe from the drop-down menu to display data for that period. Available ranges are **3 Months**, **6 Months**, and **9 Months**. By default, 3 months of data are displayed.
   - **Decoder Limit**: Specify the number of decoders to be displayed in the chart. Users can configure a range from 1 to 10 Decoders.

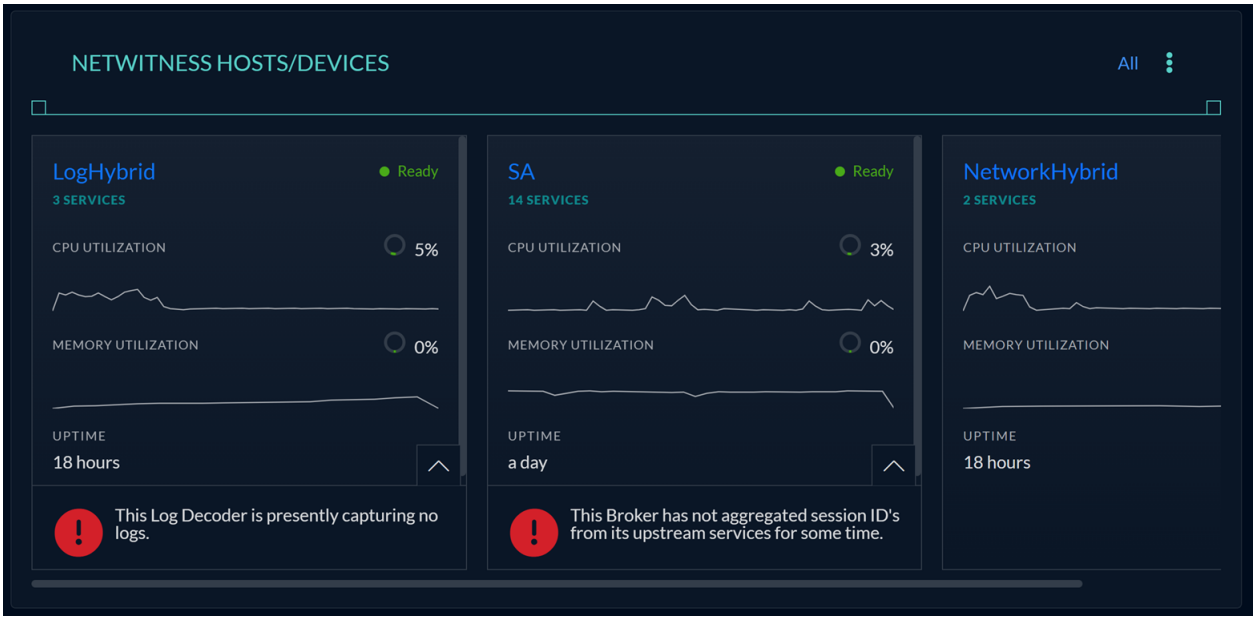
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

NetWitness Hosts/Devices

This widget shows the hosts connected to the Netwitness Platform and its CPU and memory utilization. It also displays the uptime from when the host is available and any associated active alerts. A sparkline shows the historical data and a donut chart shows the most recent data point. Also, a warning message is displayed below the uptime. Click the up-arrow button to see the detailed warning message description.

Note:
• This widget is available by default only in **Admin** view.
• To allow other users to view the widget metrics, an administrator must enable **admin-server.monitoring.read** permission on the admin server. For more information, see the Admin-server section in the "Role Permissions" topic in the *System Security and User Management Guide*.

IMPORTANT:
• Ensure that the SMS service of the Admin Server remains always online in case the SMS service goes offline, troubleshoot, and restore the service immediately. For more information on troubleshooting the SMS service, see the Troubleshooting Health & Wellness topic in the *System Maintenance Guide*.
• If there is insufficient data available for a device, such as having only one historical CPU or memory data point, the graph for that device will not be displayed.



By default, the widget shows the first three Hosts/Devices. The Hosts/Devices CPU and Memory usage and trends over time, active Services status, and active alerts, if applicable, are displayed in this widget. This extended data visibility enables effective analysis of trends and informed security decisions.

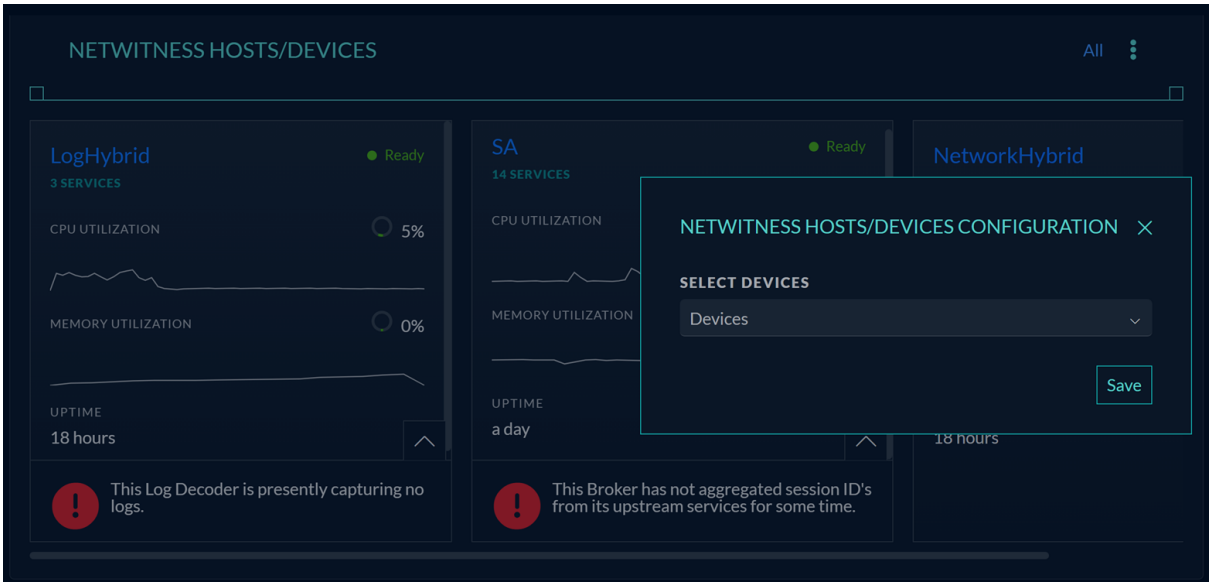
Click on the hostname to navigate to its location in the NetWitness Platform and take any remediation action if needed. The Widget interacts with the hostname, which links to the **Admin** > **Health & Wellness** > **Monitoring**. The Widget periodically updates the data without any manual intervention.

The default view shows panels with hosts with problems first. Only the permitted data is visible. A warning message is displayed for restricted data.

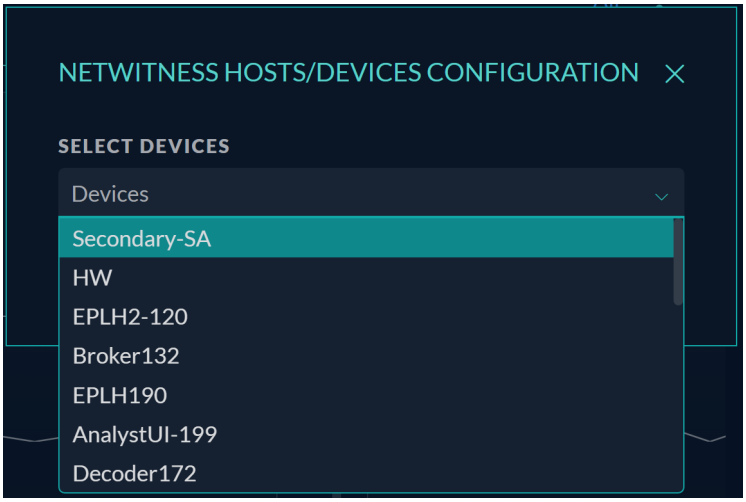
To edit the NetWitness Hosts/Devices widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.

   The **NetWitness Hosts/Devices Configuration** dialog is displayed.



2. Select the required devices from the **Select Devices** drop-down menu. Users can select all the devices available in the environment at once.

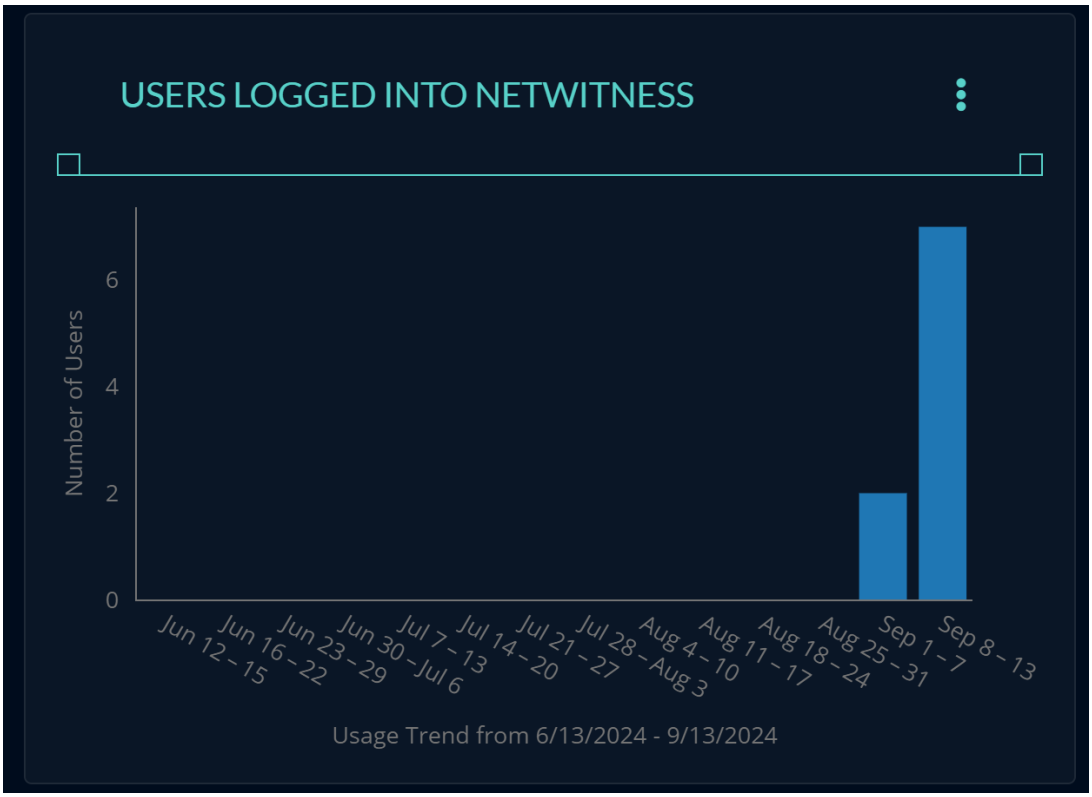


3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

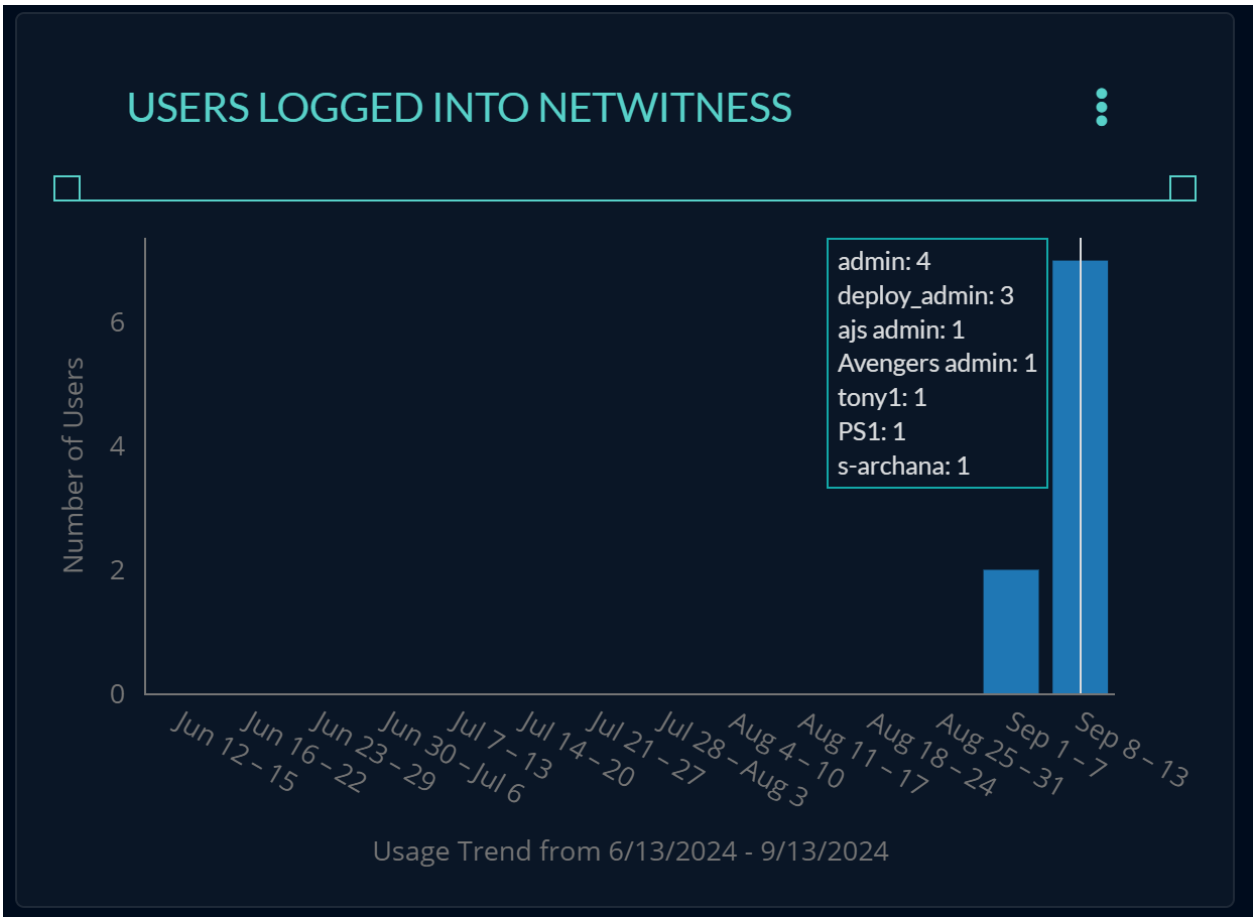
Users Logged into NetWitness

This widget helps SOC managers and administrators monitor the daily login count and usage trends. It displays the number of unique users who have accessed NetWitness using the UI or NW shell within a specific period. For example, SOC managers can analyze the number of users who logged in to NetWitness within the last three months or the last year, allowing them to make informed decisions about user access and security.

Note:
• This widget is available by default in **Admin** and **Manager** views.
• To allow other users to view the widget metrics, an administrator must enable **admin-server.userloginhistory.read** and **security-server.userloginhistory.read** permissions on the admin server and security server. For more information, see the Admin-server and Security-server section in the "Role Permissions" topic in the *System Security and User Management Guide*.



A bar chart visually presents the dataset. The vertical axis in the chart represents the count of distinct users logged into NetWitness, while the horizontal axis represents the usage trend for the period. By default, the chart displays the data for the last three months. However, users have the option to customize the widget to show data for different available time periods. The representing data is periodically updated, and when users hover their cursor over the vertical bars in the chart, a tooltip will be displayed, allowing users to view the exact names and their usage counts. The full name of the user is displayed, and if that is not available, the username will be displayed. This is only valid if they have set up their users using NetWitness. If they use Active Directory, SSO, PAM, etc., only the userIDs will be displayed.



Note:
• User logins are tracked each day by recording only one login by each user. This means that regardless of how many times a user logs in and out during a day, it will only be counted as one login for that day.
• Consider a scenario where the user has logged in three distinct days a week. When the user moves the cursor over the vertical bar, a tooltip appears that shows the number three for this user.
• The data for all the logins from the previous day will be available the following day.

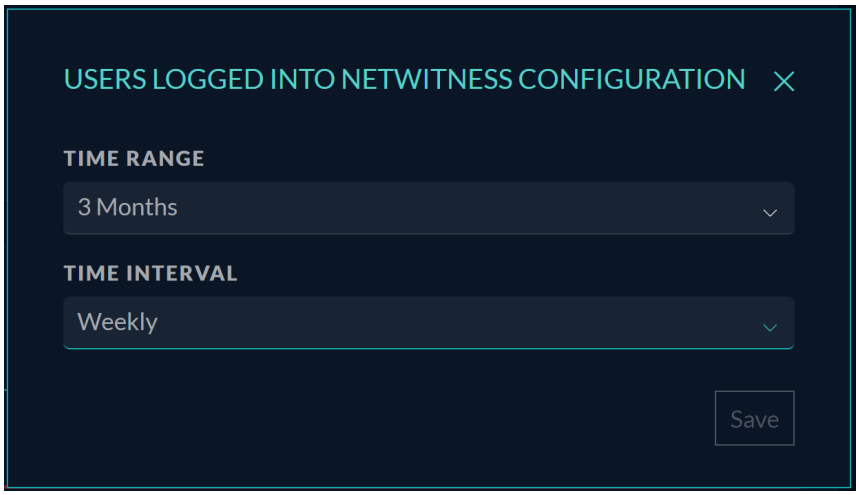
IMPORTANT: If the user sets the time range to **12** and **9** months with a **Weekly** interval, the data will be displayed for each week. However, the x-axis labels (Usage Trend) on the chart will be shown alternately. To display all labels on the x-axis, the user can increase the widget sizes. For more information on resizing the widgets, see Rearrange and Resize Widgets section in the topic Customize the Dashboard Layout.

Users can edit the existing widget at any time to change the time range or modify the time interval used by the widget, allowing users to customize it according to their preferences.

To edit the Users Logged into NetWitness widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.

   The **Users Logged into NetWitness Configuration** dialog is displayed.



2. Configure the following options based on your preference:
   - **Time Range**: Select a specific timeframe from the drop-down menu to display data for that period. Available ranges are **3 Months**, **6 Months**, **9 Months**, and **12 Months**. By default, 3 months of data are displayed.
   - **Time Interval**: Select the required time interval, either **Weekly** or **Monthly**, from the drop-down menu. Based on the selected time interval, NetWitness collects and aggregates login data for different users.
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

Global Retention

The Global Retention widget provides a comprehensive summary of the maximum retention period available for queries related to meta, logs, or packets. This widget enables analysts to avoid missing any data in their queries by indicating the lowest retention among the decoders. For example, if one decoder has 25 days of retention while the others have 30 days, the global retention would be 25 days.

Note: If you have both Log and Packet Decoders, you will see information for both packets and logs; otherwise, you will only see information for the decoder you have installed.

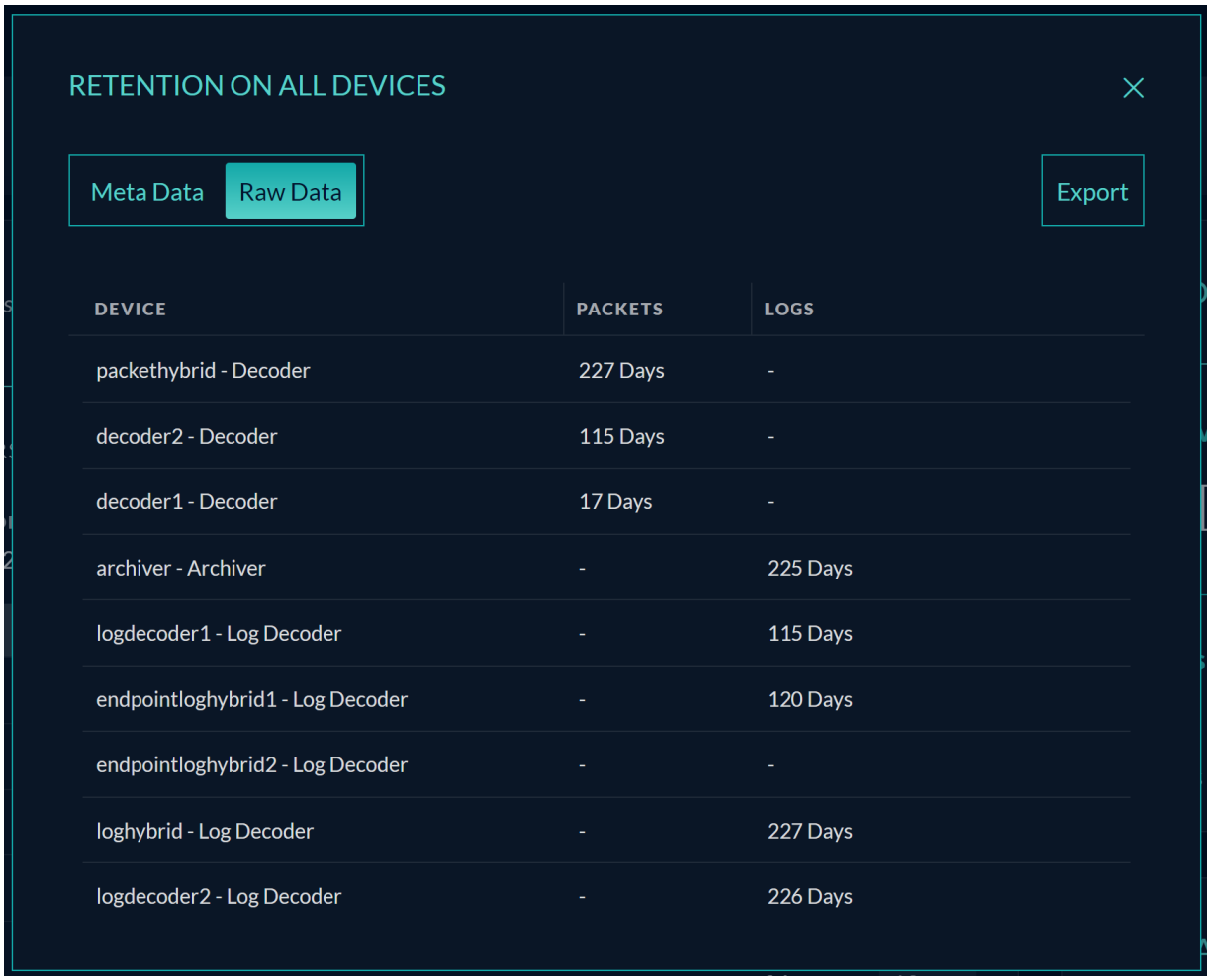
Note: This widget is available by default in **Admin** and **Analyst** views.

You can see the following information on the Global Retention widget:

- **Raw Available**: Displays the raw data available for the device with the least amount of retention data among all your devices in your environment.
- **Meta Available**: Displays the metadata available for the device with the least amount of retention data among all your Concentrators in your environment.
- **Packets** : Displays the least amount of retention (meta data) among all Packet Decoders.
- **Logs**: Displays the least amount of retention (raw data) among all Log Decoders.

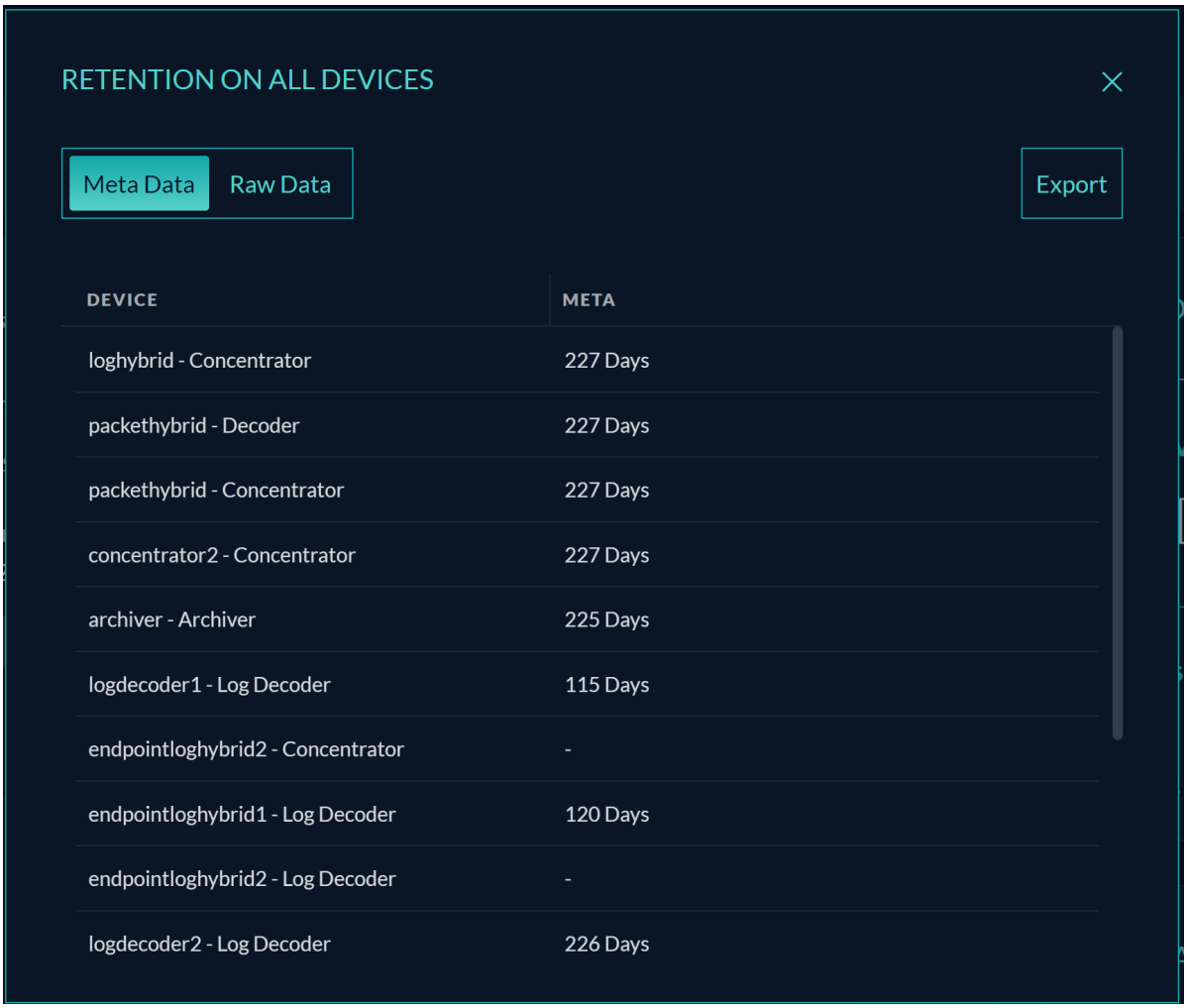
- To view the retention details of all devices, click the **All** link. The **Retention on All Devices** dialog is displayed.

  By default, the **Meta Data** option is selected. To switch to **Raw Data**, use the toggle button.



Note: The Raw Data is available only for decoders.

You can see the following information for each device in the dialog:



In the **Meta Data** tab, following information is displayed:

- **Device**: Displays the installed device type, such as Concentrator, Packet Decoder, Archiver, and Log Decoder.
- **Meta**: Displays the retention period available for metadata collected and processed for each device. For example, 227 days.

In the **Raw Data** tab, following information is displayed:

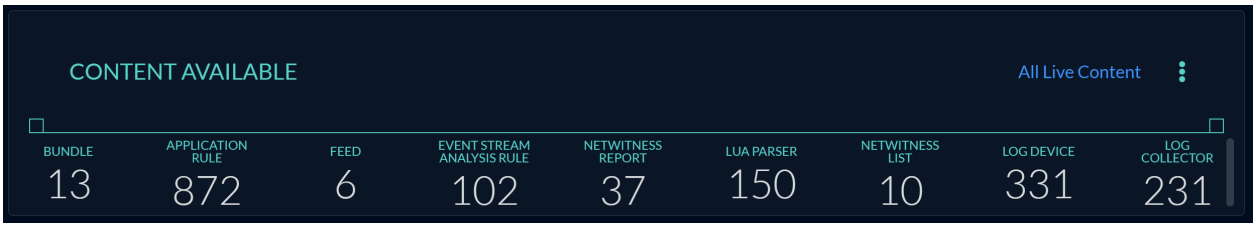
- **Device**: Displays the installed device type, such as Concentrator, Packet Decoder, Archiver, and Log Decoder.
- **Packets**: Displays the retention period available for packets that have been processed for each device. For example, 115 days.
- **Logs**: Displays the retention period available for logs data for each device. For example, 225 days
- Click **Export** to download the data in .csv format for further analysis.
- Click **X** to close the dialog.

Content Available

This widget displays the number of content available across content types such as **Bundle**, **Application Rule**, **Feed**, **Event Stream Analysis**, **NetWitness Report**, **LUA Parser**, **NetWitness List**, **Log Device**, and **Log Collector**.

Note: This widget is available by default only in **Admin** view.

The widget displays the lists containing the top 9 content types.



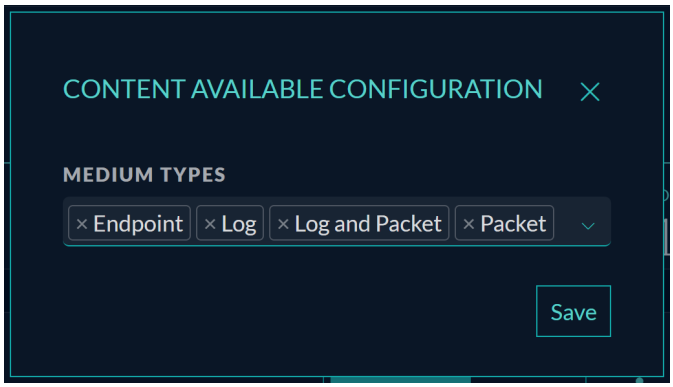
Click **All Live Content** to view the all the live content in the **Configure** > **Live Content** page.

NetWitness 12.5.1, this widget is enhanced with the new Configuration option.

To edit the Content Available widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.

   The **Content Available Configuration** dialog is displayed.



2. Configure the following options based on your preference:
   - **Medium Types**: This option sets the medium for the content type. Options include Endpoint, Log, Log and Packet, and Packet. Based on the selected medium, the widget displays the content available.
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

Mean Time to Detect (MTTD)

This widget is available by default in **Admin** and **Manager** views. For more information on the widget, see Mean Time to Detect (MTTD) section in the Manager view.

Mean Time to Resolve (MTTR)

This widget is available by default in **Admin** and **Manager** views. For more information on the widget, see Mean Time to Resolve (MTTR) section in the Manager view.

Alert Trend Over Time

This widget is available by default in **Admin** and **Manager** views. For more information on the widget, see Alert Trend Over Time section in the Manager view.

False Positives (Incidents)

This widget is available by default in **Admin** and **Manager** views. For more information on the widget, see False Positives (Incidents) section in the Manager view.

Incident Overview

This widget is available by default in **Admin** and **Manager** views. For more information on the widget, see Incident Overview section in the Manager view.

Analyst View

The Analyst Dashboard provides a high-level overview of the current threat landscape in your environment, presenting platform-wide detections and indicators generated by the NetWitness Platform. Analysts can use the dashboard to monitor the severity and frequency of security events, identify potential threats, and drill down into the details for further investigation. The analyst view consists of several out-of-the-box widgets that display different aspects of the data, such as:

- Overview
- Mitre ATT&CK Overview
- Top Suspicious Endpoints
- Top Suspicious Files
- Events
- Global Retention
- Top Suspicious Users
- Top Discovered Assets
- FirstWatch Threat Logic & Live Content Updates
- Latest FirstWatch Blogs
- Incidents and Alerts

The Analyst dashboard is updated frequently and shows the most recent data. You can also customize the dashboard by rearranging the widgets according to your preferences.

Overview

This Overview widget is displayed as the top most widget in the Analyst view and it consists of the following 5 default cards..

- **Incidents**: This card displays the total number of incidents created in the last 24 hours.
- **New Incidents**: This card displays the total number of incidents which are still in the New state for the last 24 hours.
- **Closed Incidents**: This card displays the total number of incidents which are closed in the last 24 hours.
- **Alerts**: This card displays the total number of alerts created in the last 24 hours.
- **Critical Alerts**: This card displays the total number of critical alerts created in the last 24 hours.

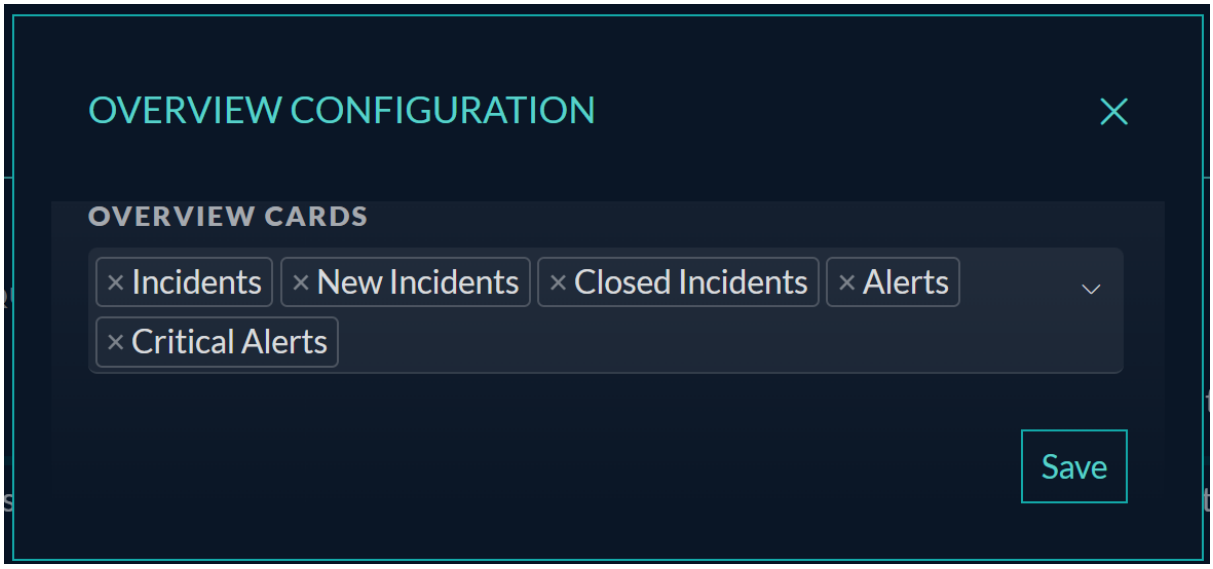
By default, this widget displays the last 24 hours data when you log in to the NetWitness Platform.

You can edit the Overview widget at any time and add additional cards. However, you can have a maximum of 5 cards displayed at once.

To edit the Overview Widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.

   The **Overview Configuration** dialog is displayed.



2. Select the required cards from the **Overview Cards** drop-down menu.
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

Mitre ATT&CK Overview

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. This dashboard includes the tactics and techniques to describe adversarial actions and behaviors. Techniques refer to specific actions an attacker might take, while tactics refer to the different phases of attacker behavior.

From NetWitness 12.5 or later, NetWitness introduces the new **MITRE ATT&CK Overview** widget, which considers the data such as log, endpoint, and packet and active content deployed in your environment, such as Application rules and ESA rules to help you view relevant MITRE ATT&CK content for these rules and shows the complete coverage. This MITRE ATT&CK Overview helps analysts to view detailed information on the Tactics, Techniques, and Sub-Techniques associated with content in one place, not only can you filter on specific techniques to see how well you are covered for each, but you can also filter on specific source data type to see the coverage they give you. Thus eliminating the need to visit Mitre's website for ATT&CK information.

IMPORTANT: MITRE ATT&CK Overview coverage is based on the rules available in CCM. If CCM is not enabled, you cannot view content coverage on the MITRE ATT&CK Overview widget. For more information, see Centralized Content Management for NetWitness.

To access the MITRE ATT&CK Overview

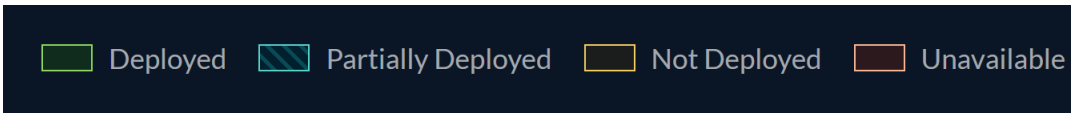
1. On the top-right corner, select either **Analyst View** or **Manager View** from the drop-down menu.

   The **MITRE ATT&CK Overview** widget is displayed.

The tactics, techniques, and sub-techniques information displayed are from the MITRE ATT&CK framework.

For example, In the Execution tactic, out of the 14 techniques available. NetWitness covers 8 techniques and does not cover 6 techniques.

Tactic and Technique available states



- **Deployed** - Technique and sub-techniques have content and are deployed on services. These contents are identified by the green color. The technique and sub-technique contents are in a **Deployed** state in the following scenarios:

  There is no content in the technique, and all sub-techniques are deployed on services.

  - Both the technique and sub-techniques having contents are deployed.
  - The technique has content and is deployed but its sub-techniques do not have any content available.

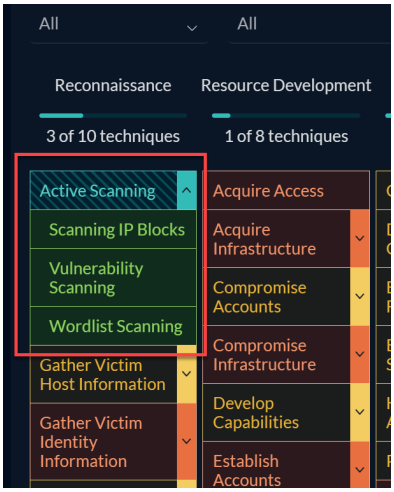
- **Partially Deployed** - All techniques and sub-techniques have content, but only a few are deployed on services. These contents are identified by the teal color. The technique and sub-technique contents are in a **Partially Deployed** state in the following scenarios:
  - The technique has content available and is deployed, and all sub-techniques or only a few sub-techniques are deployed to services.
  - The technique has content available and is deployed, and only a few sub-techniques have content available.
  - There is content available but not deployed for a given technique, and only a few or all related sub-techniques are deployed on services.

- **Not Deployed** - Content is available for a given technique or sub-technique but is currently not deployed on the services. These contents are identified by the yellow color. The technique and sub-technique contents are in a **Not Deployed** state in the following scenarios:
  - The technique has no content, and all sub-techniques or a few sub-techniques have content.
  - There is content available for the technique, and some or all of its sub-techniques also have content.
  - Technique has content, and sub-techniques have no content.

- **Unavailable** - If there are no contents available for a given technique or sub-technique. These contents are identified by the orange color. The technique and sub-technique contents are in a **Unavailable** state in the following scenarios:
  - Both techniques and sub-techniques have no content available.

The **Mitre ATT&CK Overview** widget is frequently updated with the most recent data. To view the recent data, you must log out of the UI and log in again.

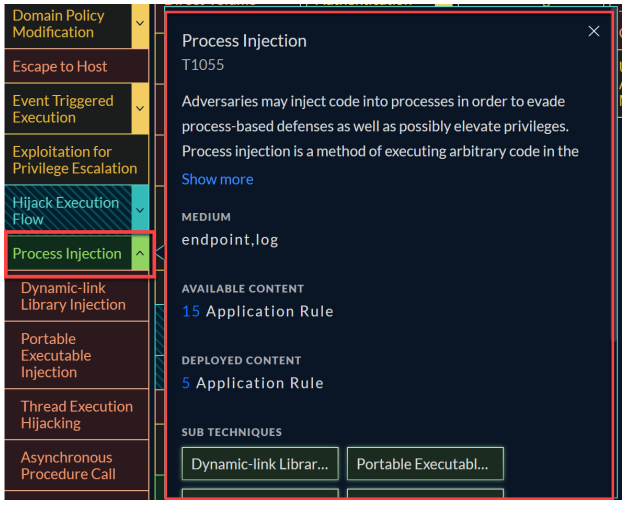
2. To view the sub-techniques, click (**down arrow**) button, which expands and shows the number of sub-techniques associated with a particular technique. For example, for the technique of **Active Scanning**, the related sub-techniques Scanning IP Blocks, Vulnerability Scanning, and Wordlist Scanning are displayed.



3. Click on any technique For example, **Process Injection**. A pop-up window is displayed, which shows the following information:

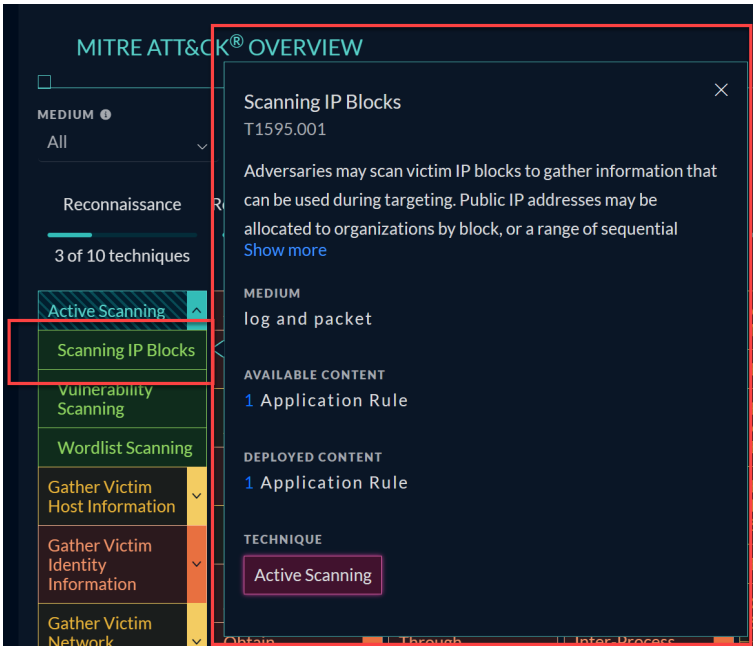
   - Displays the name of the Technique
   - Displays the Mitre Technique ID associated.
   - Displays a brief description of the technique.
   - Displays the type of medium for the technique. For example, endpoint, log.
   - Displays the number of available contents. For example, the Application Rule.
   - Displays the number of deployed contents.
   - Displays the sub-techniques associated with the particular technique. Clicking on the sub-technique will open another pop-up window with related information.

- Click **X** to close the pop-up window.



4. Click on any sub-technique. A pop-up window is displayed, which shows the following information:
   - Displays the name of the sub-technique.
   - Displays the Mitre sub-technique ID.
   - Displays a brief description of the sub-technique.
   - Displays the type of medium for the technique. For example, log and packet.
   - Displays the number of available contents. For example, the Application Rule.
   - Displays the number of deployed contents.
   - Displays the associated technique. Clicking on the technique name will show the related technique panel with all the information.

- Click **X** to close the pop-up window.



5. Select the data from the **Medium** drop-down menu to filter by the data type from which the metadata is generated. By default, **All** is selected, and you can select either **Log**, **Packet**, **Endpoint**, or **Log and Endpoint** based on your coverage.
6. Select the content from the **Content Type** drop-down menu to filter by content type. By default, **All** is selected, but based on your coverage, you can select either the **Application Rule** or **Event Stream Analysis Rule**.
7. Select the **Expand All Sub Techniques** checkbox to view all the sub-techniques available at once.

Top Suspicious Endpoints

The Top Suspicious Endpoints widget displays a lists of the top 25 top suspicious endpoints by default detected based on the highest risk score and Operating system (Windows, Linux, and Mac).

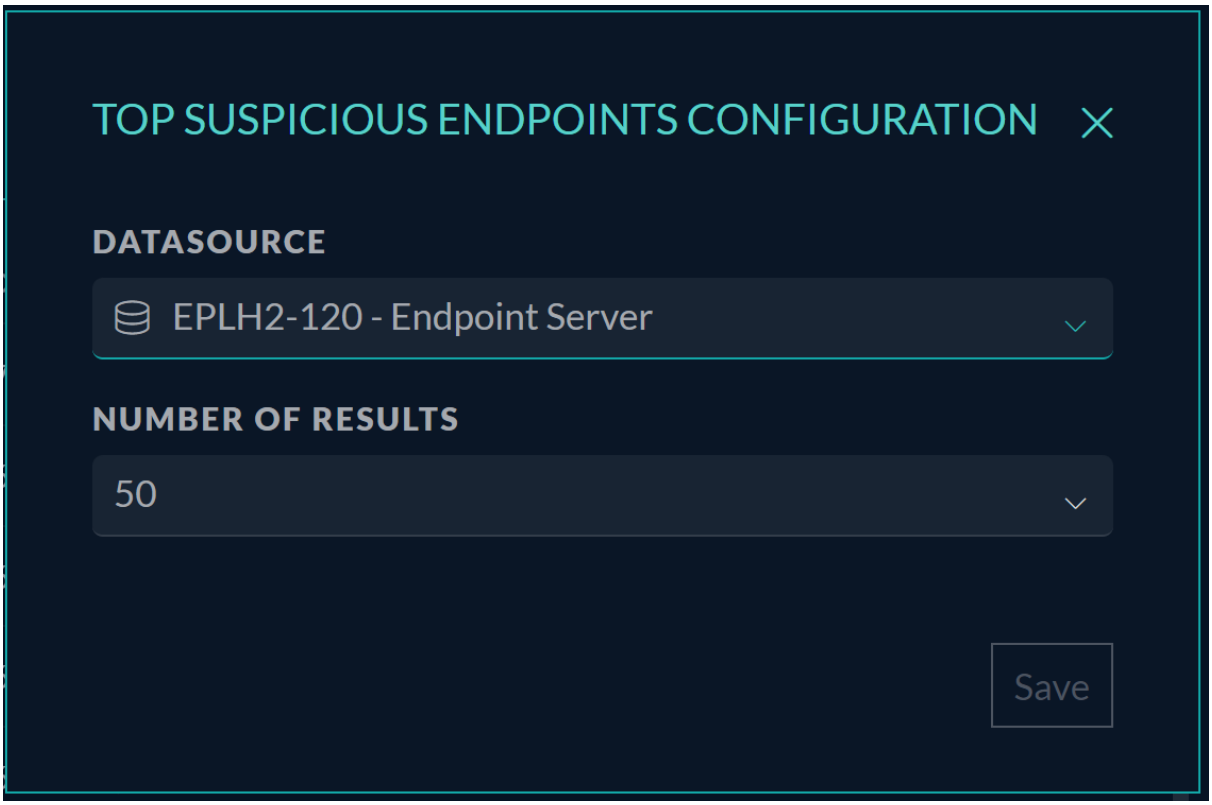
Note:
- This widget is available by default in **Analyst** view.
- To allow other users to view the widget metrics, an administrator must enable **endpoint-server.agent.read** and **endpoint-server.agent.manage** permissions on the endpoint server and **endpoint-broker-server.agent.read** and **endpoint-broker-server.agent.manage** permissions on the endpoint broker. For more information, see the Endpoint-server and Endpoint-broker-server sections in the "Role Permissions" topic in the *System Security and User Management Guide*.

Each Endpoint is displayed with the following information:

- **Risk Score**: Displays the risk score of the endpoint based on the severity and frequency of the alerts generated by the endpoint. The risk score ranges from 0 to 100, with higher scores indicating higher risk. The endpoints are sorted in descending order by their risk scores.
- **Host Name**: Displays the name of the host as it appears on the network. Clicking on a specific Hostname takes you to the **Hosts Details** view, where you can see all the events and alerts generated for this host.
- **Operating System**: Displays the Operating system on which the agent is running (Linux, Windows, or Mac).
- **IP Address**: Displays the IP address of the endpoint.
- **Last Active User**: Displays the name of the user who logged in to the endpoint most recently.
- **Location**: Displays the geographic location of the endpoint based on its IP address. For example, **United States**.
- Click the **All** option to view all the risky endpoints on the **Hosts** > **Endpoints** view.
- Use the pagination options to navigate and view the Endpoints data seamlessly.

To edit the Top Suspicious Endpoints widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.
   The **Top Suspicious Endpoint Configuration** dialog is displayed.



2. Configure the following options based on your preference:
   - **Datasource**: Select the required Endpoint Server or Endpoint Broker Server from the drop-down menu.
   - **Number of Results**: Select the required number of results from the drop-down menu. Available number of results are **25**, **50**, **75**, and **100**. By default, 25 number of results are displayed.

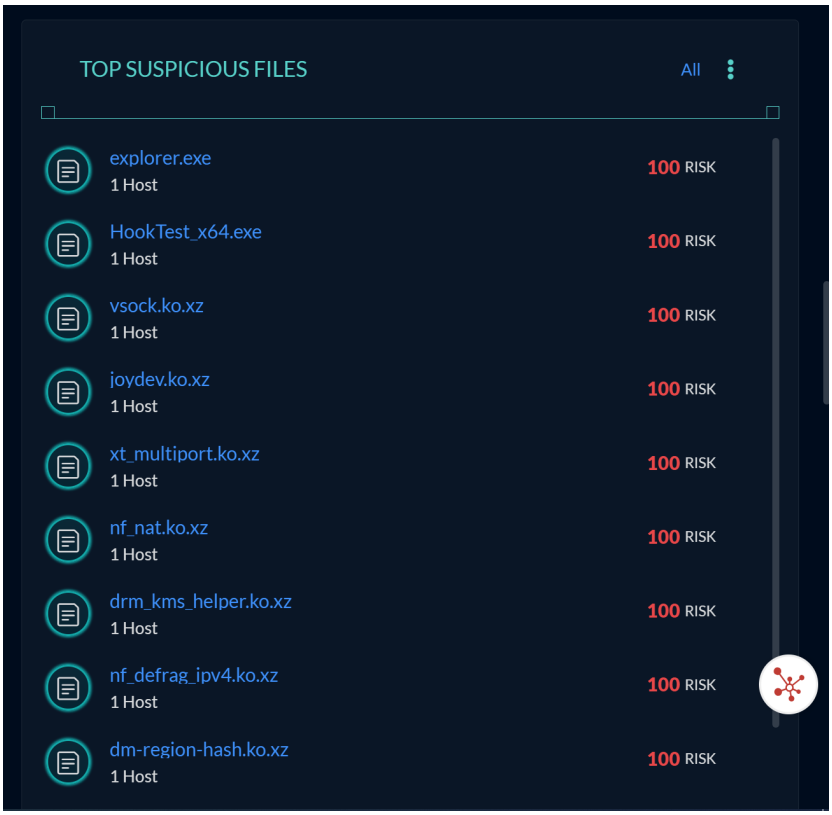
     Based on the selected datasource and number of results, NetWitness displays the top suspicious endpoint data.
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

For more information on Hosts, see *NetWitness Endpoint User Guide*.

Top Suspicious Files

The Top Suspicious Files widget displays a lists of the top 25 suspicious risky files by default with the highest risk score detected in your endpoint.

Note:
- This widget is available by default in **Analyst** view.
- To allow other users to view the widget metrics, an administrator must enable **endpoint-server.agent.read** and **endpoint-server.agent.manage** permissions on the endpoint server and **endpoint-broker-server.agent.read** and **endpoint-broker-server.agent.manage** permissions on the endpoint broker. For more information, see the Endpoint-server and Endpoint-broker-server sections in the "Role Permissions" topic in the *System Security and User Management Guide*.



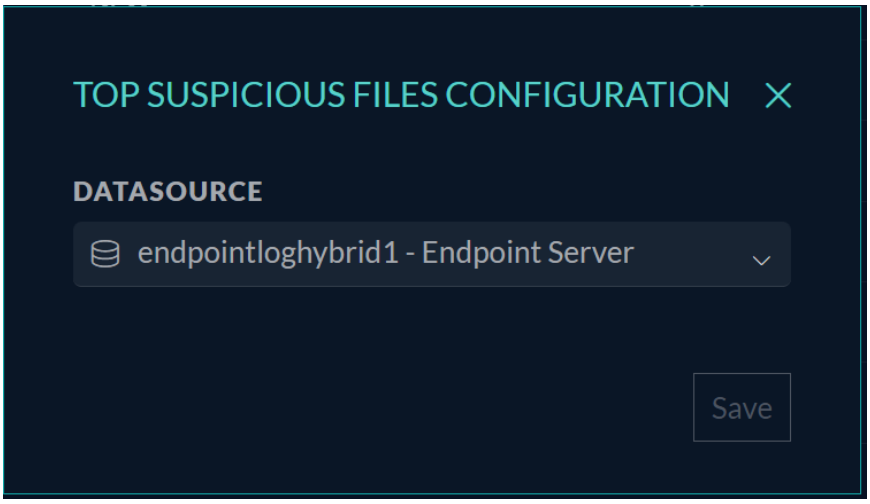
Each File is displayed with the following information:

- Displays the file type and number of hosts affected by the suspicious file. Clicking on a specific file link navigates you to the **Files Details** view, where you can see all the events and alerts generated for this file.
- Displays the risk score for each file and is based on the file analysis results. The risk score ranges from 0 to 100, with higher scores indicating higher risk. The files are sorted in descending order by their risk scores.
- Click the **All** option to view all the risky files on the Files view.

To edit the Top Suspicious Files widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.

   The **Top Suspicious Files Configuration** dialog is displayed.



2. **Datasource**: Select the required Endpoint Server or Endpoint Broker Server from the drop-down menu.

   Based on the selected datasource, NetWitness displays the top suspicious files data.

3. Click **Save** to persist the changes made to the configuration.

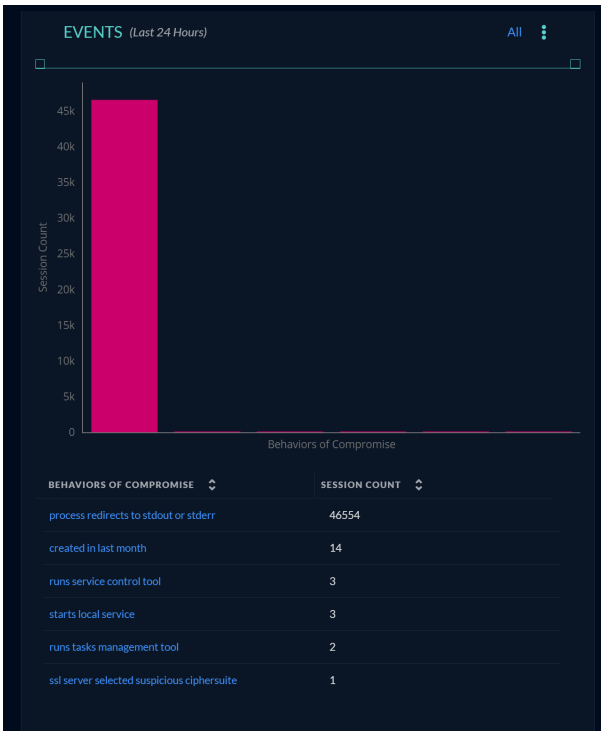
4. Click **X** to close the Configuration dialog.

For more information on Files, see *NetWitness Endpoint User Guide.*

Events

The Behavior of Compromise Events widget displays the top events that occurred for a particular meta query at a specific time in your environment. This widget helps analysts quickly identify and prioritize the most relevant and suspicious events and drill down into the details of each event.

Note:
- This widget is available by default in the **Analyst** view.
- To allow other users to view the widget metrics, an administrator must enable these combination of permissions **investigate-server.*** and **accessInvestigationModule** or **investigate-server.predicate.read**, **investigate-server.event.read**, and **accessInvestigationModule** permissions on the investigate server. For more information, see the Investigate-server section in the "Role Permissions" topic in the *System Security and User Management Guide*.



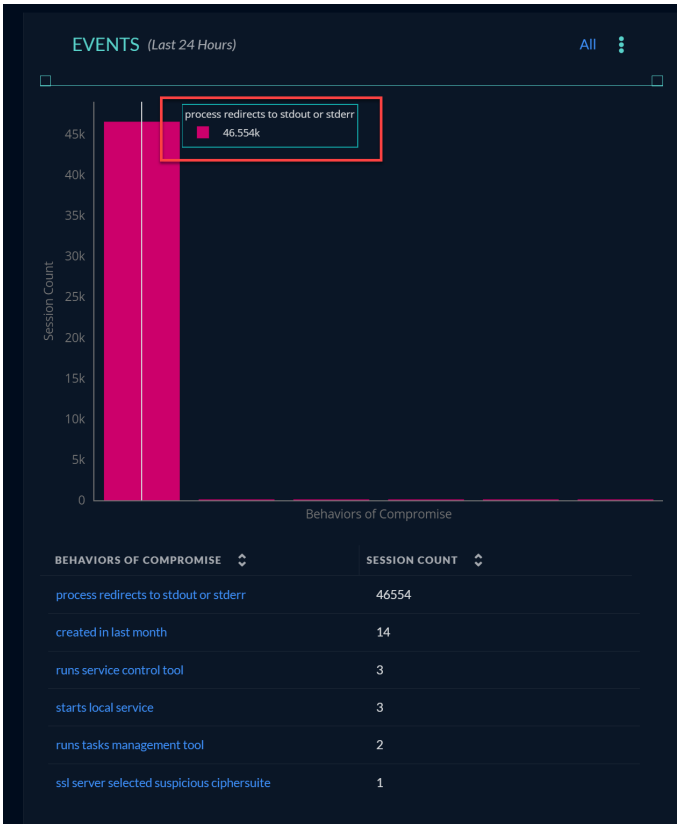
The vertical axis in the chart represents the session count, while the horizontal axis represents the Behavior of Compromise Meta value, which can be configured based on user preference. By default, the chart displays the data for the last 24 hours. However, users have the option to customize the widget to show data for different available time periods.

Note: If the data for the Meta value is not available for the specified time range, no data will be displayed on the chart.

The Events widget displays the following information:

- Displays the events for a meta query, boc exists, which indicates possible malicious activities. For example, Behaviors of Compromise (BOC).
- Displays the Events data in a Bar or Donut chart. The specific meta value and related session count are displayed when you hover over a bar or donut chart.

- Displays the number of sessions available for each meta.



Analysts can perform the following actions:

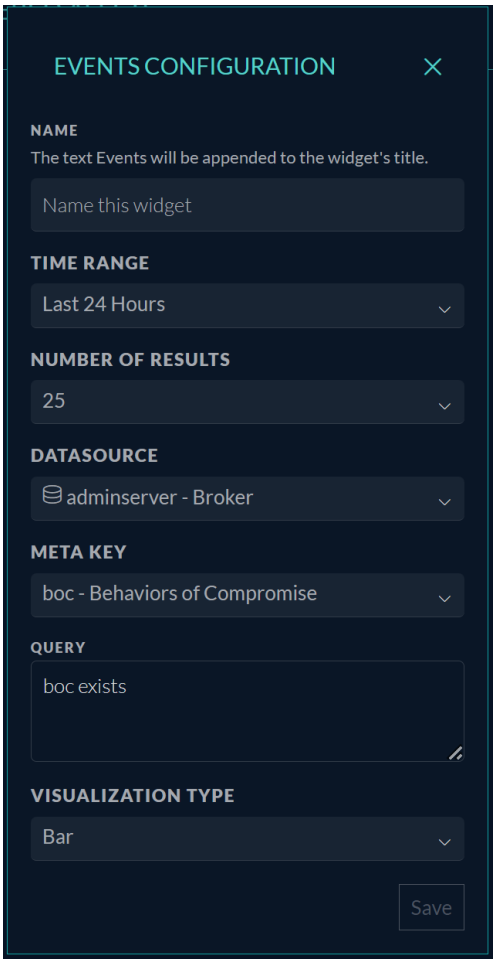
- Click on a specific meta value link in the table (for example, attack) that navigates you to **Investigate** > **Events** view, where the **boc exists And boc = 'attack'** query filter is applied to display all the events associated with the query in the events table.
- Click the **All** link to navigate to the **Investigate** > **Events** view with a boc exists query filter applied. This will display all the related events available in the events table.
- You can sort either by meta values or session count. By default, events are sorted with meta values with high session counts in descending order.
- Use the vertical scroll bar to view various meta values.
- You can navigate between pages using the page navigation options and view all the Events data seamlessly.

You can edit the existing widget at any time to update its preferences, change the meta key, or modify the query used by the widget, allowing users to customize it according to their preferences.

To Edit the Events Configuration widget

1. Click the three-dot ( ) icon located in the upper-right corner of the widget and click **Configuration**.

   The **Events Configuration** dialog is displayed.



2. Configure the following options in the **Events Configuration** dialog:

   - **Name**: Enter a unique name for the widget. The name can include alphabets, numbers, spaces, and special characters, such as _ - ( ) [ ].

     Note: The text **Events** will be appended to the widget's title. For example, if you enter the name behavior of compromise, the widget's title will be displayed as Events - Behavior of Compromise.

   - **Time Range**: Select a specific timeframe from the drop-down menu to display data for that period. You can select any time range from L**ast 5 Minutes** to **Last 7 Days**. By default, 24 hours of data are displayed.

     Note: The time range will be displayed next to the widget's title based on the configured time frame.

   - **Number of Results**: Select the number of required results from the drop-down menu. The available results are **25**, **50**, **75**, and **100**. By default, 25 results are selected.

   - **Data Source**: Select the source of the data to use for the widget. You can use either **Broker** or **Concentrator** from the drop-down list.

   - **Meta Key**: Select the required Meta Key available for the service from the drop-down list. For example, **boc – Behaviors of Compromise.**

- **Query**: Enter a valid query to filter for results in the Events view. For example, **boc exists**.

  Note: You can increase the text area size by placing the cursor in the bottom corner of the text box on the right-hand side and dragging the box.

- **Visualization Type**: Select the required visualization type from the drop-down menu. You can select either a **Bar** or a **Donut** chart.

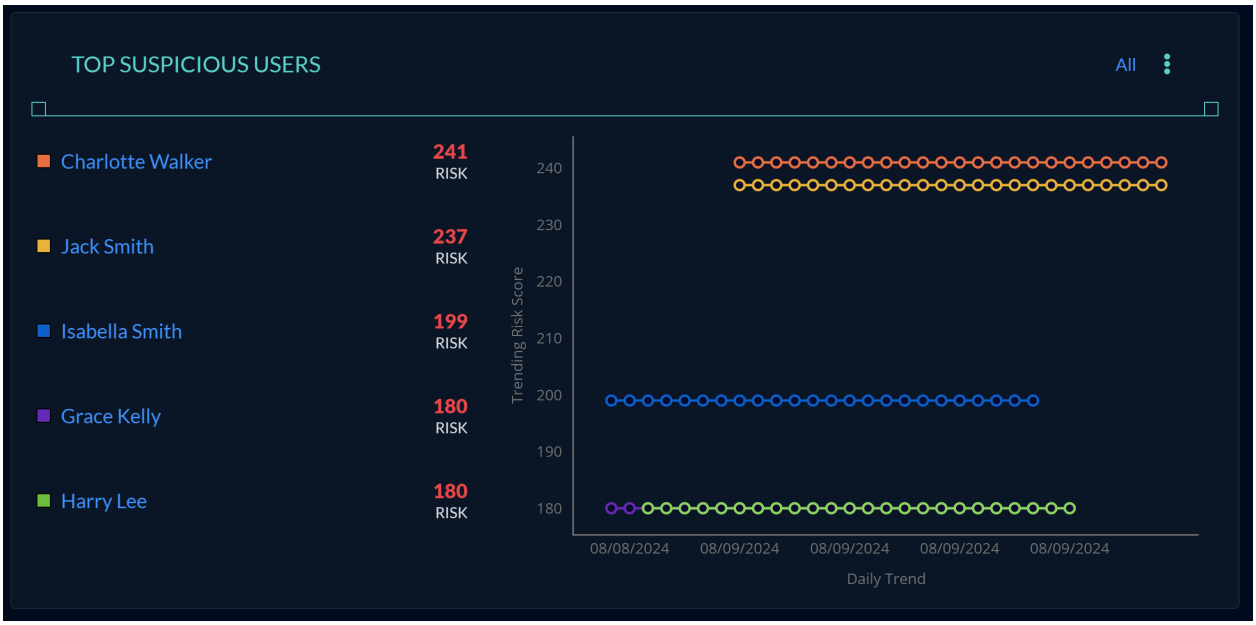
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

Global Retention

For more information, see Global Retention widget in Admin view section.

Top Suspicious Users

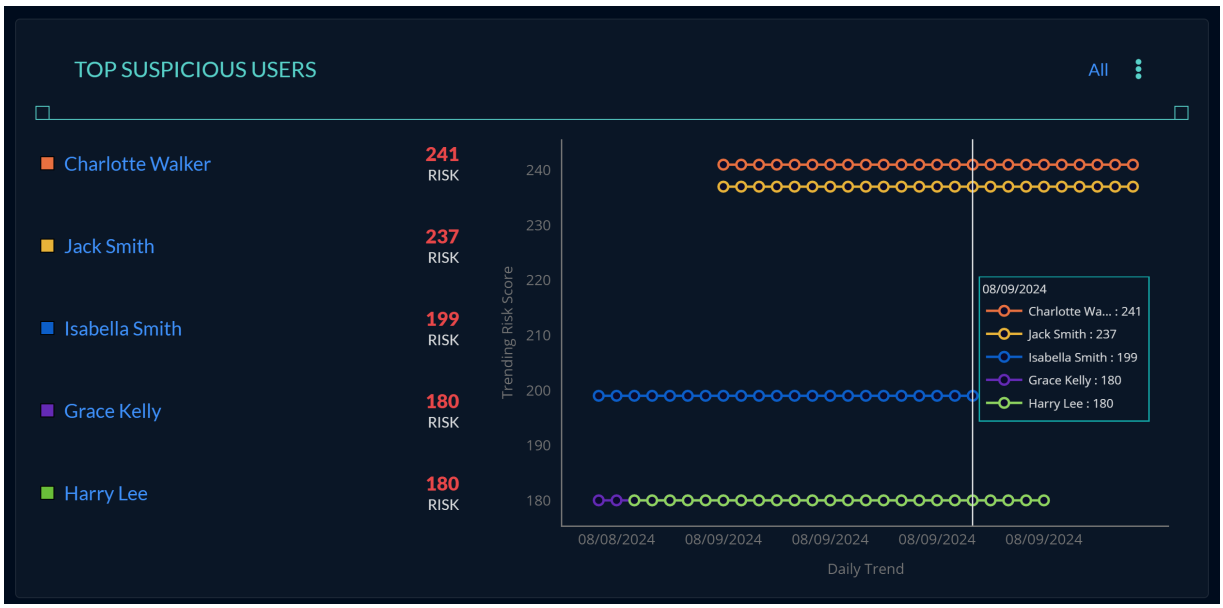
The Top Suspicious Users widget lists the top 5 Suspicious users sorted by highest risk scores. This widget provides visibility into user behavior patterns across an organization. This data helps you to identify, track, and alert on anomalous user behavior that may indicate malicious activity, such as abnormal login time or performed unauthorized actions.



Note:
- The Top Suspicious Users widget only displays data from your on-premises UEBA server, which must be installed and configured. For more information on installation, see Installation Tasks in the *NetWitness UEBA Standalone Installation Guide*.
- The user must contain both the Analyst and UEBA Analyst roles to access the widget metrics. For more information, see "Assign User Access to UEBA" topic in the *NetWitness UEBA Configuration Guide*.

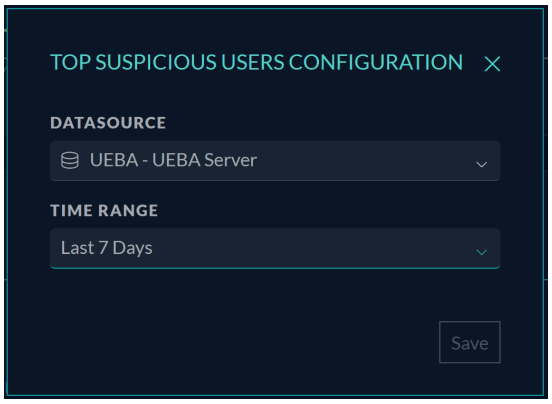
You can see the following information in the Top Suspicious Users widget:

- View the top suspicious users sorted by highest risk scores in descending order.
- Click on a specific user link, for example, **Jack Smith** which will navigate you to the user's details view, where you can see all the alerts and modeled behaviors associated with the user.
- Each user is assigned a specific color code.
- The chart shows the distribution of users by their risk level, which is indicated by a color code. You can see the behavior pattern for each user weekly and track how each user's risk level has changed over time.
- Click the **All** link option to view all the users listed on the **Users** > **Entities** view.



To Edit the Top Suspicious Users widget

1. Click the three-dot ( ) icon located in the upper-right corner of the widget and click **Configuration**. The **Top Suspicious Users Configuration** dialog is displayed.



2. Configure the following options based on your preference:

- **Datasource**: Select an UEBA Server from the drop-down menu.
- **Time Range**: Select the required time range from the drop-down menu. Select **Last 24 Hours** to view the daily trend of suspicious users and select **Last 7 Days** to view the weekly trend of suspicious users.

  Based on the selected datasource and time range, NetWitness displays the top suspicious users data.

3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

Top Discovered Assets

The Top Discovered Assets widget displays a lists of the top 25 risky assets by default detected in your environment based on their enterprise network exposure rank. This enables the analysts to gain a comprehensive understanding of an asset's significance within the enterprise network and identify potential risks and threats associated with the asset that require immediate action.

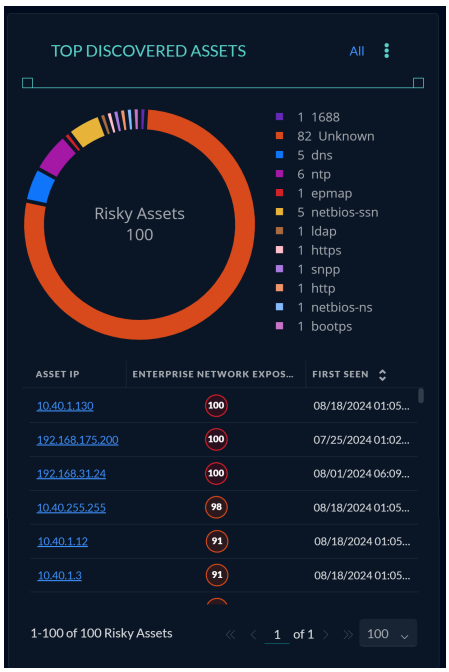
Note: An Insight sensor and Cloud Connector sensor must be installed and configured in your environment to receive the asset's data. For more information on installing the sensors, see topics Install Insight Sensor and Install the Cloud Connector Sensor.

Note:
- This widget is available by default in **Analyst** view.
- To allow other users to view the widget metrics, an administrator must enable **cloud-connector-server.networkasset.read** and **cloud-connector-server.query.read** permissions on the Cloud-connector-server. For more information, see the Cloud Connector-Server section in the "Role Permissions" topic in the *System Security and User Management Guide*.

You can see the following information in the Top Discovered Assets widget:

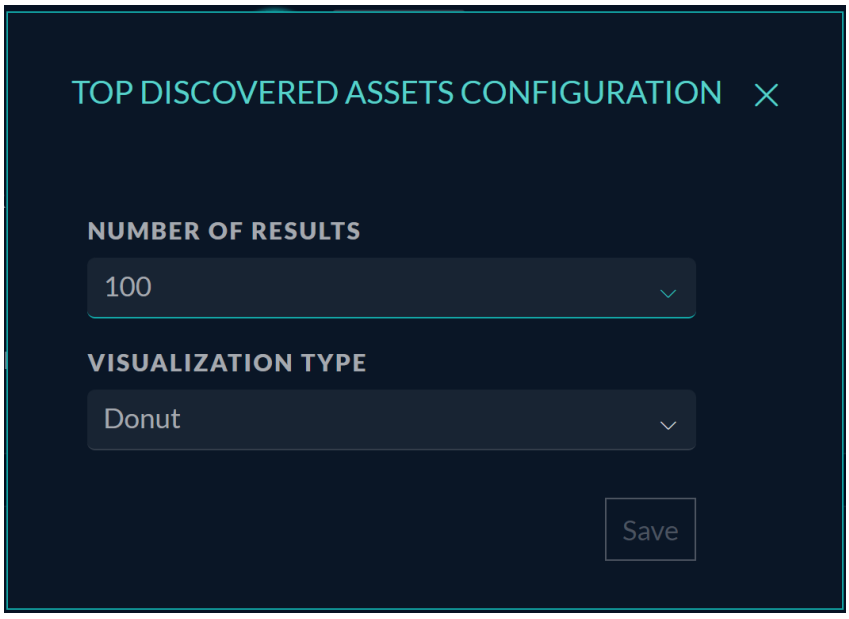
- The Asset IPs are sorted by higher enterprise network exposure rank in descending order. You can sort them in either ascending or descending order.
- Displays the timestamp when the asset was first observed.
- Click the **All** link in the assets widget to view all the assets listed in the **Hosts** > **Assets** view. This view provides other important information for the asset, such as asset type, peer network exposure, etc.
- The donut chart gives the breakdown of the asset category type. You can hover over the donut chart to see the asset category type. For example, unknown,dns, ntp, etc.
- Use the vertical scroll bar to view various Asset IPs.
- When you click on any asset IP address link, it takes you to the **Hosts** > **Assets** view in a new tab using the asset IP address as the filter, sorted in descending order by time.

- Use the pagination options to navigate and view the assets data seamlessly.



To Edit the Top Discovered Assets widget

1. Click the three-dot ( ) icon located in the upper-right corner of the widget and click **Configuration**. The **Top Discovered Assets Configuration** dialog is displayed.



2. Configure the following options based on your preference:
   - **Number of Results**: Select the required number of results from the drop-down menu. Available number of results are **25**, **50**, **75**, and **100**. By default, 25 number of results are displayed.

- **Visualization Type**: Select a visualization type either **Donut** or **Bar** from the drop-down menu.

  Based on the selected visualization type and number of results, NetWitness Insight displays the top discovered assets data.

3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

FirstWatch Threat Logic & Live Content Updates

This widget lists the latest content uploaded by NetWitness and the Community.

The FirstWatch Threat Logic & Live Content Updates widget lists the latest 12 content uploaded by NetWitness and Community. The list is sorted based on the content uploaded date. Each content is displayed with an icon along with a tag to indicate if it is a Community or NetWitness content, content updated time and name of the content.

Note: NetWitness content and Community content will have different icons.

You can perform following actions on the widget:

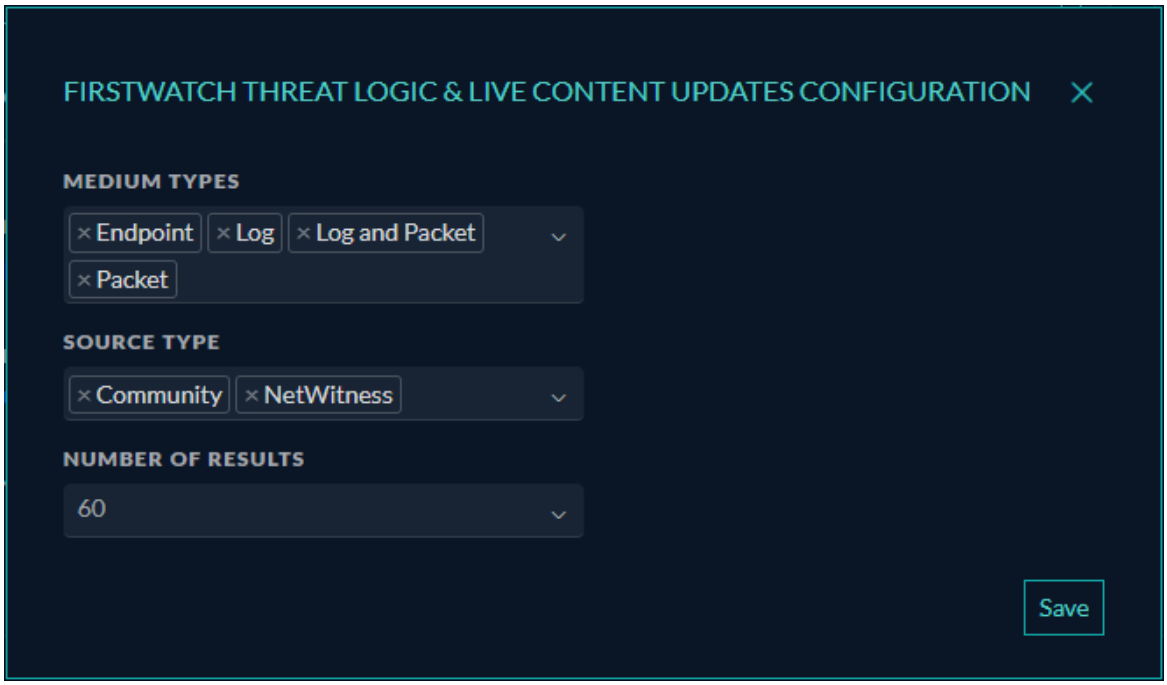
- A link to the content details is provided through the title of the content. Click the link to view the details of the content.
- Click **All** to view all the uploaded content in the **Configure > Live Content** page.

In NetWitness 12.5.1, this widget is enhanced with the new Configuration option.

To Edit the FirstWatch Threat Logic & Live Content Updates

1. Click the three-dot ( ) icon located in the upper-right corner of the widget and click **Configuration**.

   The **Configuration** dialog is displayed.

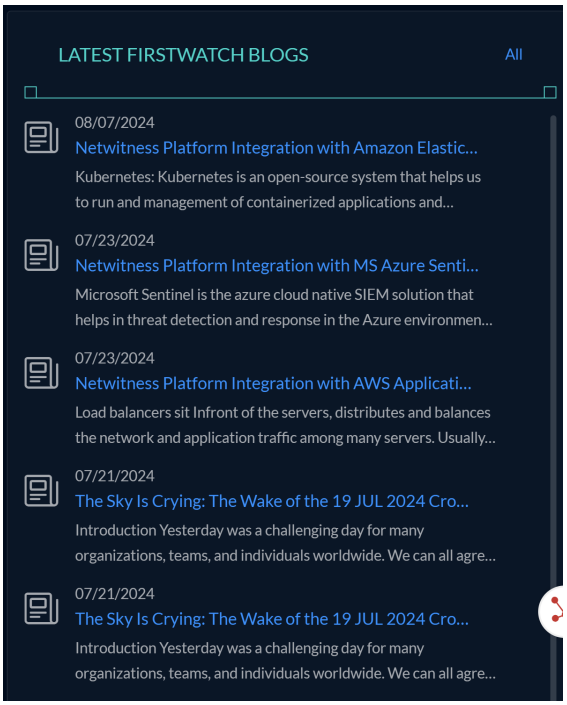


2. Configure the following options based on your preference:
   - • **Medium Types**:This option sets the medium for the content type. Options include Endpoint, Log, Log and Packet, and Packet.
   - • **Source Type**: Select the required Community or NetWitness source type from the drop-down menu.
   - **Number of Results**: This option sets the number of results to be displayed on the widget. Available number of results are 12, 28, 44, and 60. By default, 12 number of results are displayed.

     Based on the selected medium types, source type, and number of results, NetWitness displays the FirstWatch Threat Logic & Live Content Updates data.
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

Latest FirstWatch Blogs

The **Latest FirstWatch Blogs** widget that lists the latest 10 blogs uploaded to the NetWitness Community portal. The list is sorted based on blog creation date. Each blog is displayed with icon along with title and paragraph of the blog.



You can perform following actions on the widget:

- A link to the blog details is provided through the title of the blog. Click the link to view the details of the blog.
- Click **All** to view all the blogs in the NetWitness Community portal.

Incidents and Alerts

For more information, see Incident Overview widget in Manager view section.

Manager View

This view shows the widgets and associated data that only Managers and Administrators can access.

The Manager dashboard consists of several out-of-the-box widgets that display different aspects of the data, such as:

- Top Bar
- MITRE Overview
- Mean Time to Detect (MTTD)
- Mean Time to Resolve (MTTR)
- Incident Trend Over Time
- Alert Trend Over Time

- Incident SLAS
- Incident Status by Priority
- False Positives (Incidents)
- Incident Flow
- Team Workload
- Incident Overview by Owner
- Incident Overview

Top Bar

This widget is displayed as the top most widget in the Manager view and it consists of the following 5 sections (also known as cards):

- **Mean Time to Detect**: This section displays the mean time to detect incidents in Respond.
- **Mean Time to Resolve**: This section displays the mean time to resolve incidents in Respond.
- **Incidents**: This section displays the total number of incidents created in the last 24 hours.
- **New Incidents**: This section displays the total number of incidents which are still in the New state for the last 24 hours.
- **Closed Incidents**: This section displays the total number of incidents which are closed in the last 24 hours.

Note: By default, this widget displays the last 24 hours data when you log in to the NetWitness Platform.

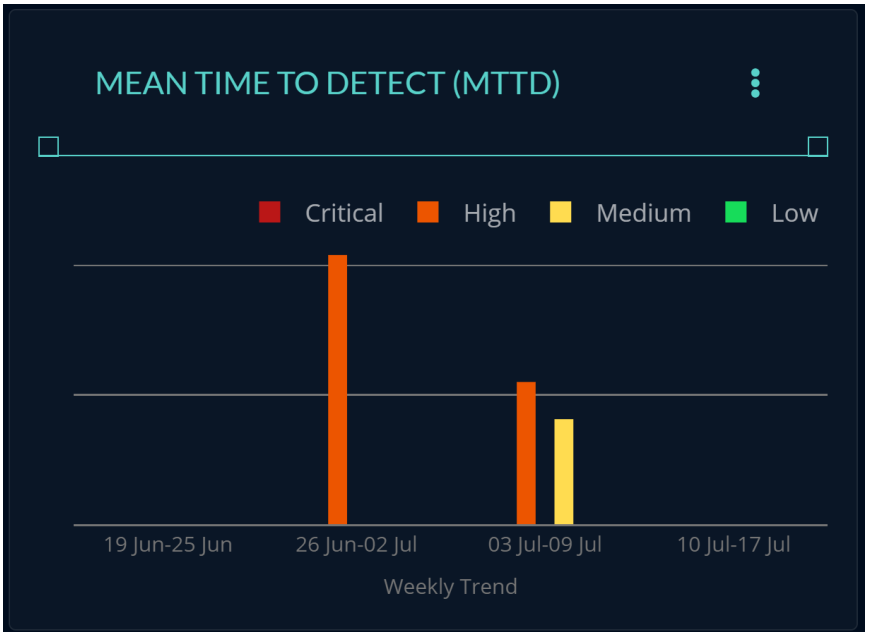
MITRE Overview

For more information on the **MITRE Overview** widget, see **Widgets Displayed in the Analyst** view.

Mean Time to Detect (MTTD)

This widget displays the mean/average time to detect incidents in Respond. The time passed between the assignment of an incident and the closure of the incident is calculated and displayed. It enables the Managers to make informed decisions regarding the incidents detected, time taken by analysts' to resolve the incidents, and how the platform performs over time.

A stacked bar graph visually presents the dataset. By default, it showcases the values for MTTD of incidents over a time range of 30 days on a weekly trend basis. However, users have the option to configure the widget to display the data for a maximum of 90 days. Each bar segment in the chart is color-coded to represent a specific Priority, as indicated by the chart legend. Users have the option to configure the Priority. The bar segments are arranged such that the mean time to detect values of critical incidents occupies the first position, followed by others in descending order. Users can also set the Time Unit based on Minutes, Hours, or Days.



Placing the cursor over a graph bar will display a tooltip allowing the user to view the exact values of MTTD for each incident priority represented.

To edit the Mean Time to Detect (MTTD) widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.

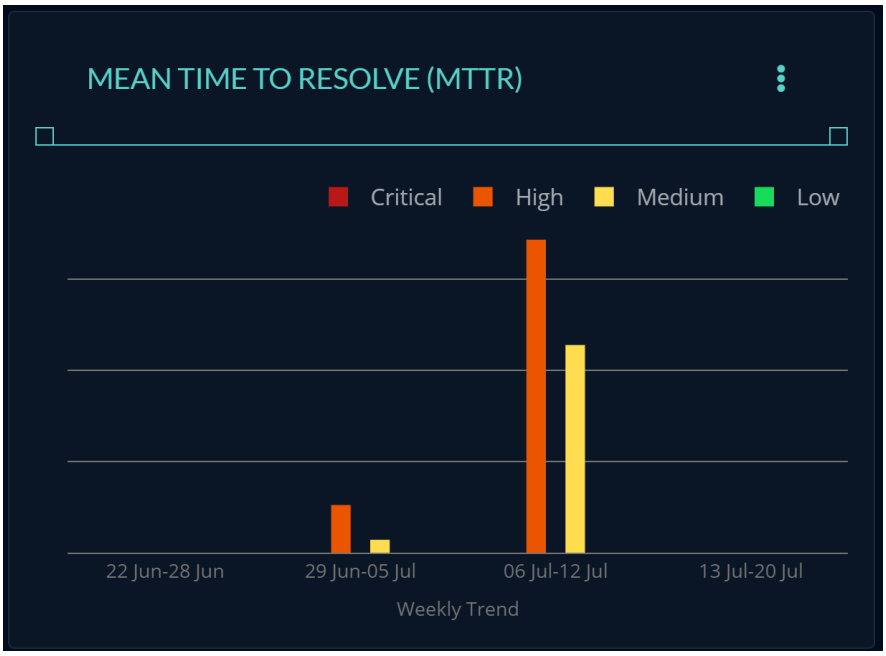
   The **Mean Time to Detect (MTTD) Configuration** dialog is displayed.

2. Configure the following options based on your preference:
   - **Time Range**: This option sets the date range. Options include Last 30 Days or Last 90 Days.
   - **Time Unit**: This option sets the time unit. Options include Minutes, Hours, and Days.
   - **Priority**: This option sets the priority. Options include Low, Medium, High, and Critical. Based on the selected Priority, the chart displays the mean time taken to detect.
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

Mean Time to Resolve (MTTR)

This widget displays the mean/average time to resolve incidents in Respond. The time taken to resolve/close an incident since it was created is calculated and displayed. It enables the Managers to respond to an incident, of varying priorities and see the how effective the incident response process is performing over time.

A stacked bar graph visually presents the dataset. By default, it showcases the values for MTTR of critical incidents over a time range of 30 days on a weekly trend. However, users have the option to configure the widget to display the data for a maximum of 90 days. Each bar segment in the chart is color-coded to represent a specific Priority, as indicated by the chart legend. Users have the option to configure the Priority. The bar segments are arranged such that the mean time to resolve values of critical incidents occupies the first position, followed by others in descending order. Users can also set the Time Unit based on Minutes, Hours, or Days.



Placing the cursor over a graph bar will display a tooltip allowing the user to view the exact values of MTTR for each incident priority represented.

To edit the Mean Time to Resolve (MTTR) widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.

   The **Mean Time to Resolve (MTTR) Configuration** dialog is displayed.

2. Configure the following options based on your preference:
   - **Time Range**: This option sets the date range. Options include Last 30 Days or Last 90 Days.
   - **Time Unit**: This option sets the time unit. Options include Minutes, Hours, and Days.

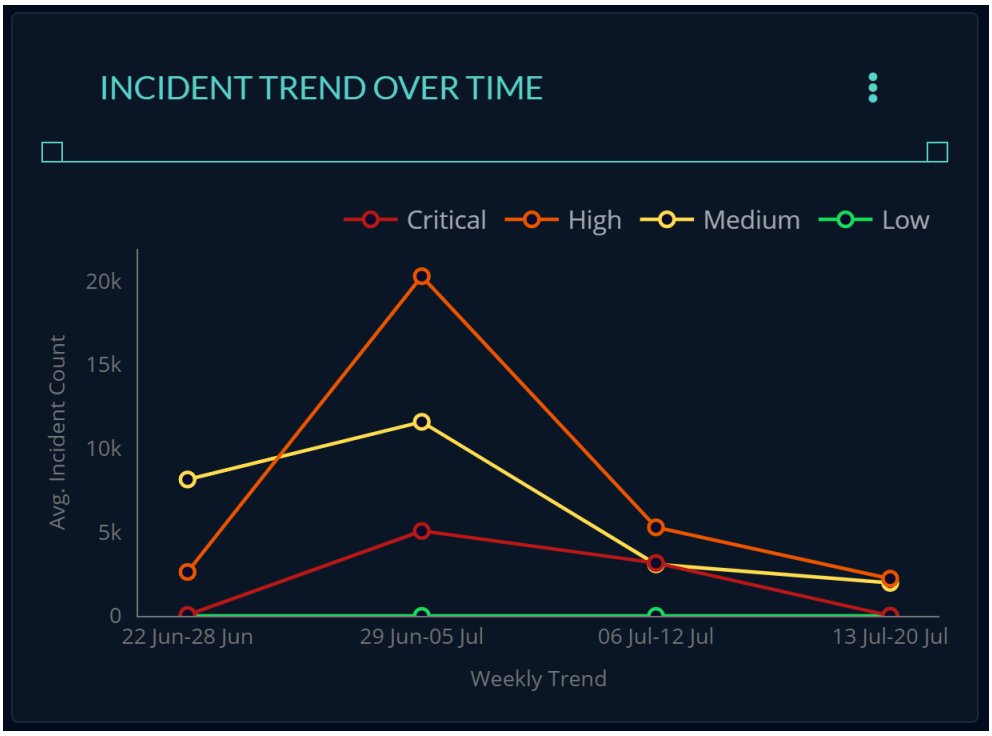
- **Priority**: This option sets the priority. Options include Low, Medium, High, and Critical. Based on the selected Priority, the chart displays the mean time taken to resolve.

3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

Incident Trend Over Time

This widget displays the average number of incidents created each week based on their priority. The default settings display Critical and High priority incidents. It enables the Managers to effectively analyze and process the changing trends and make informed security decisions.

A line graph visually presents the dataset. By default, it showcases the values for Incident Trend Over Time of critical and high incidents over a time range of 4 weeks on a weekly trend. However, users have the option to set the time filter to display the data for a maximum of 90 days. Each line segment in the chart is color-coded to represent a specific Priority, as indicated by the chart legend. Users have the option to configure the Priority of choice to show up on the graph. The vertical axis shows the average incident count, while the horizontal axis shows the weekly trend.



Placing the cursor over a graph line will display a tooltip allowing the user to view the exact values of average incident count for each incident priority represented in that displayed week.

To edit the Incident Trend Over Time widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.

   The **Incident Trend Over Time Configuration** dialog is displayed.

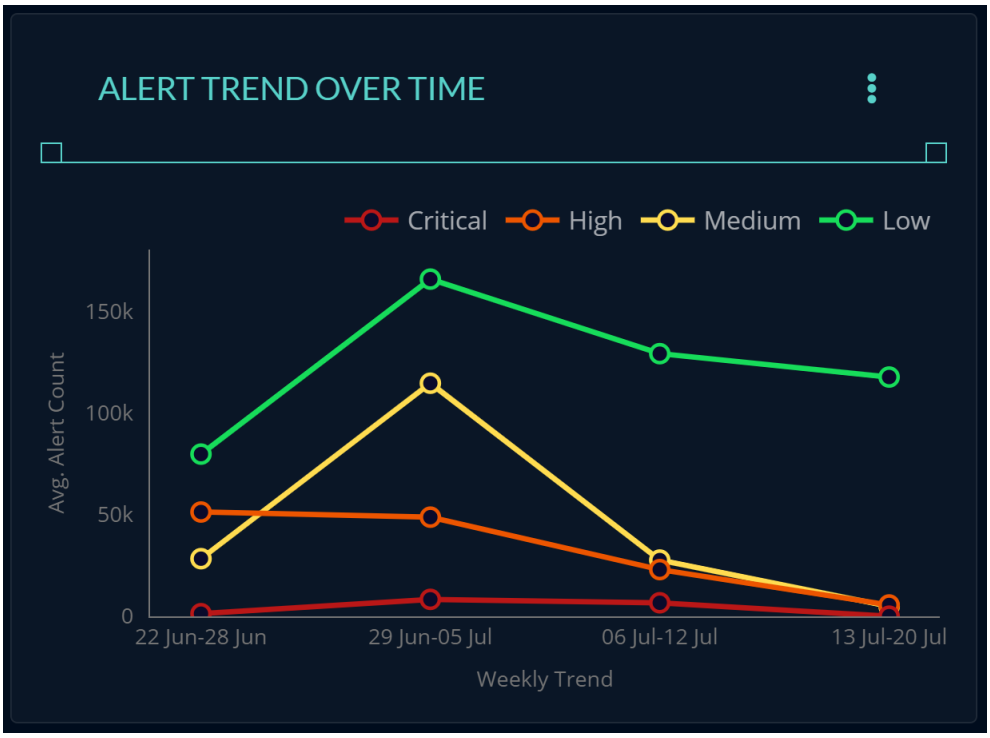
2. Configure the following options based on your preference:
   - **Priority**: This option sets the priority. Options include Low, Medium, High, and Critical. Based on the selected Priority, the chart displays the incident trend over time.
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

Alert Trend Over Time

This widget displays the average number of alerts created each week based on their severity. The default settings display Critical and High priority alerts. The last 4 weeks data is displayed in this widget. It enables the Managers to effectively analyze and process the changing trends of alerts created over time.

A line graph visually presents the dataset. By default, it showcases the values for Alert Trend Over Time of critical and high alerts over a time range of 4 weeks on a weekly trend. However, users have the option to set the time filter to display the data for a maximum of 90 days. Each line segment in the chart is color-coded to represent a specific severity, as indicated by the chart legend. Users have the option to configure the severity.

The vertical axis shows the average alert count, while the horizontal axis shows the weekly trend.



Placing the cursor over a graph line will display a tooltip allowing the user to view the exact values of average alert count for each level of alert severity represented in that displayed week.

To edit the Alert Trend Over Time widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.

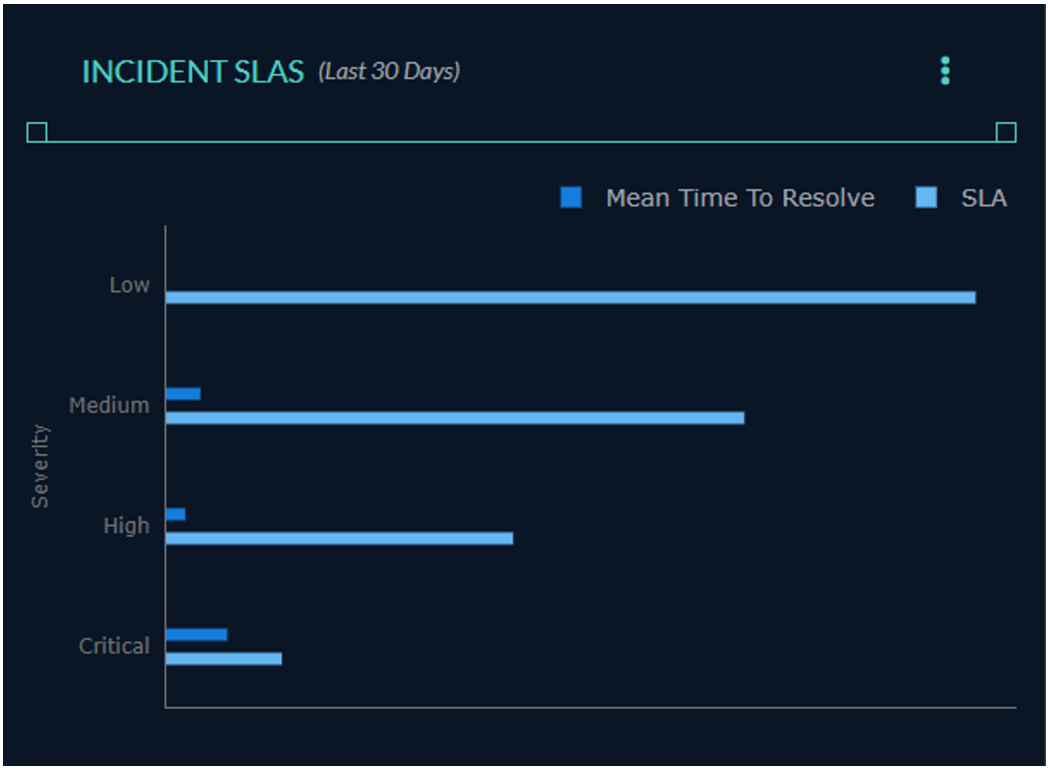
   The **Alert Trend Over Time Configuration** dialog is displayed.

2. Configure the following options based on your preference:
   - **Priority**: This option sets the severity. Options include Low, Medium, High, and Critical. Based on the selected severity, the chart displays the alert trend over time.
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

Incident SLAS

This widget displays the average time to close/resolve an incident versus the Service Level Agreement (SLA). It enables the Managers to analyze and determine if the incidents are resolved within the committed SLA.

A stacked bar graph visually presents the dataset. By default, it showcases the mean time to resolve and the SLA over a time range of 30 days for the selected priority. However, users have the option to configure the widget to display the data for a maximum of 90 days. The selected time range is displayed next to the widget name. Each bar segment in the chart is color-coded to represent the mean time to resolve and the SLA, as indicated by the chart legend. Users also have the option to configure the Time Unit, Priority and the SLA configuration.

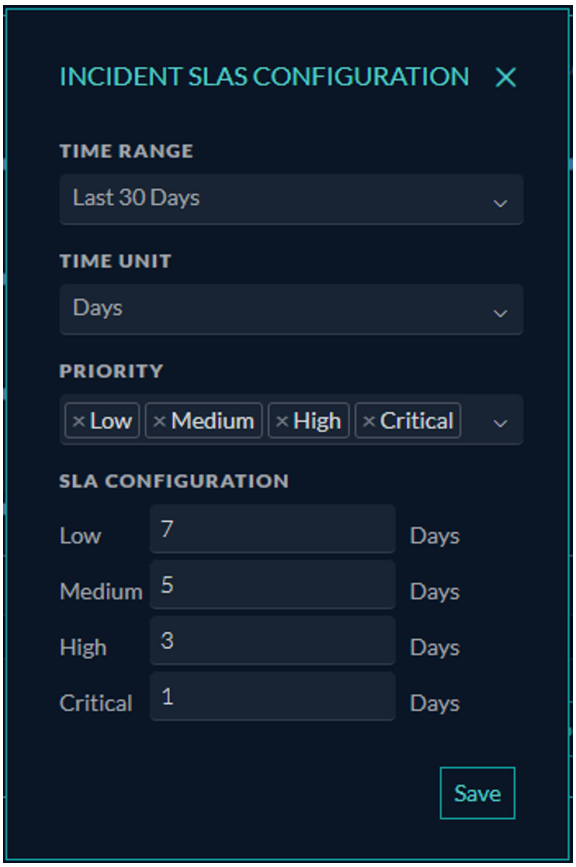


Placing the cursor over a graph bar will display a tooltip allowing the user to view the exact values of MTTR vs the SLA.

To edit the Incident SLAS widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.

   The **Incident SLAS Configuration** dialog is displayed.



2. Configure the following options based on your preference:
   - **Time Range**: This option sets the date range. Options include Last 30 Days or Last 90 Days.
   - **Time Unit**: This option sets the time unit. Options include Minutes, Hours, and Days.
   - **Priority**: This option sets the priority. Options include Low, Medium, High, and Critical.
   - **SLA Configuration**: This option sets the SLA Configuration based on the selected Time Unit for each Priority. Users can enter the preferred time unit to view the SLA values for the incidents.
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

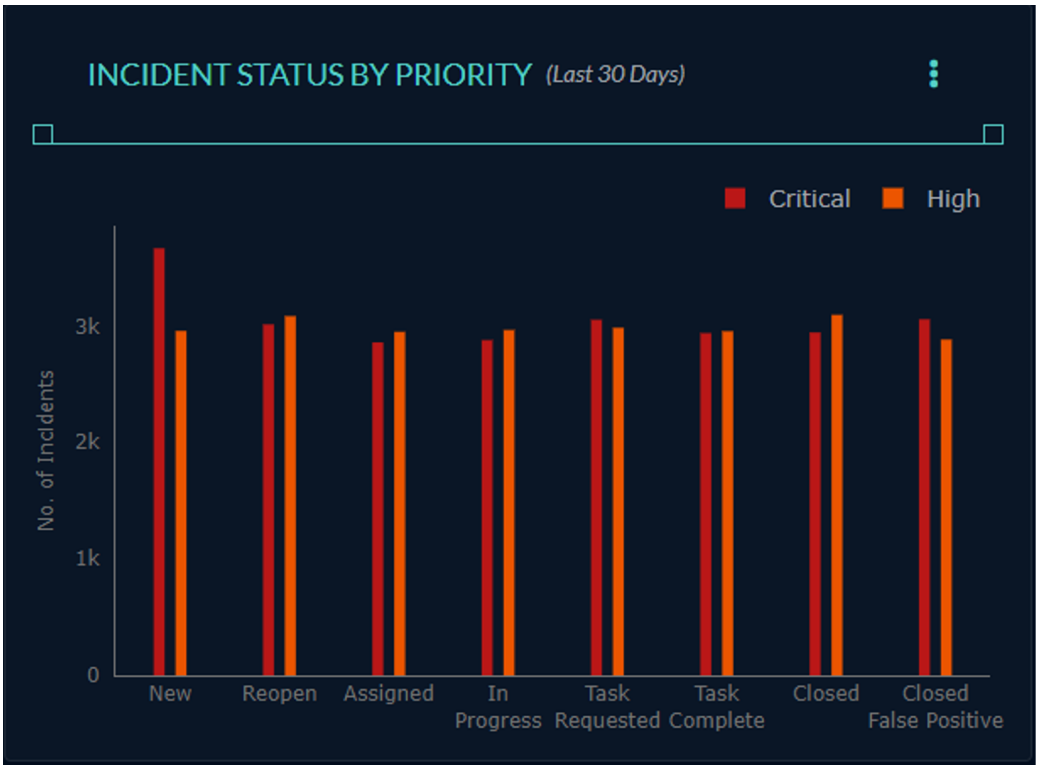
Note: When using this feature for the first time, you must configure the SLA Configuration here and save it to view this widget.

Incident Status by Priority

This widget displays the status of the actual number of incidents based on their priority. It enables the Managers to view the exact status of the incidents over time and follow up to its closure.

A stacked bar graph visually presents the dataset. By default, it showcases the status by priority of critical and high incidents over a time range of 30 days. However, users have the option to configure the widget to display the data for a maximum of 90 days. The selected time range is displayed in front of the widget name. Each bar segment in the chart is color-coded to represent a specific Priority, as indicated by the chart legend. Users have the option to configure the priority and the status.

The vertical axis shows number of incidents, while the horizontal axis shows the incident status.

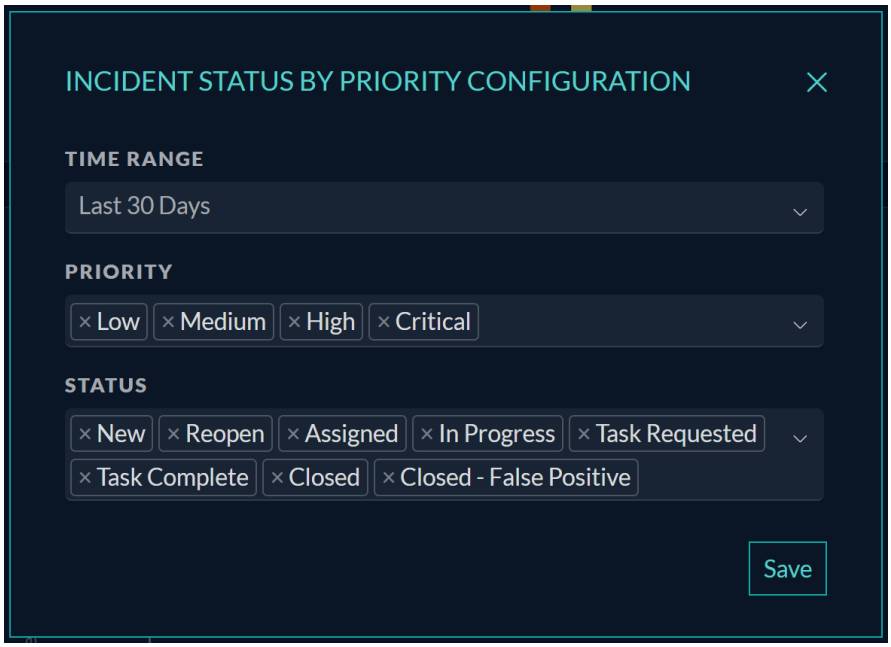


Placing the cursor over a graph bar will display a tooltip allowing the user to view the exact values of incident based on the selected status.

To edit the Incident Status by Priority widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.

   The **Incident Status by Priority Configuration** dialog is displayed.



2. Configure the following options based on your preference:
   - **Time Range**: This option sets the date range. Options include Last 24 hours, Last 7 Days, Last 30 Days or Last 90 Days.
   - **Time Unit**: This option sets the time unit. Options include Minutes, Hours, and Days.
   - **Priority**: This option sets the priority. Options include Low, Medium, High, and Critical.
   - **Status**: This option sets the incident status. Options include New, Reopen, Assigned, In Progress, Task Complete, Task Requested, Closed, and Closed False Positive.
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

False Positives (Incidents)

This widget displays the average number of False Positives (Incidents) closed among the total number of incidents closed. It enables the Managers to analyze and identify the false positives out of the total incidents closed.

A stacked bar graph visually presents the dataset. By default, it showcases the values for total incidents and false positives incidents over a time range of 30 days on a weekly trend. However, users have the option to configure the widget to display the data for a maximum of 90 days. Each bar segment in the chart is color-coded to represent the total incidents and false positives, as indicated by the chart legend.

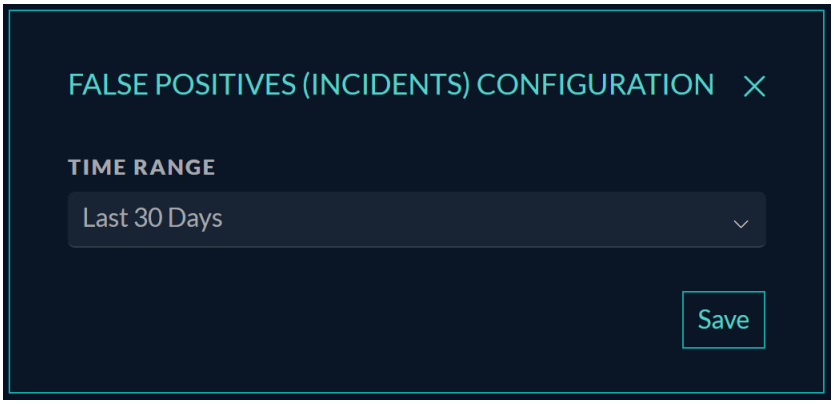
The vertical axis shows average incident count (mean calculated over the week), while the horizontal axis shows the days on a weekly basis.

Placing the cursor over a graph bar will display a tooltip allowing the user to view the exact values of total incidents and false positives for the selected time range.

To edit the False Positives (Incidents) widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.

   The **False Positives (Incidents) Configuration** dialog is displayed.



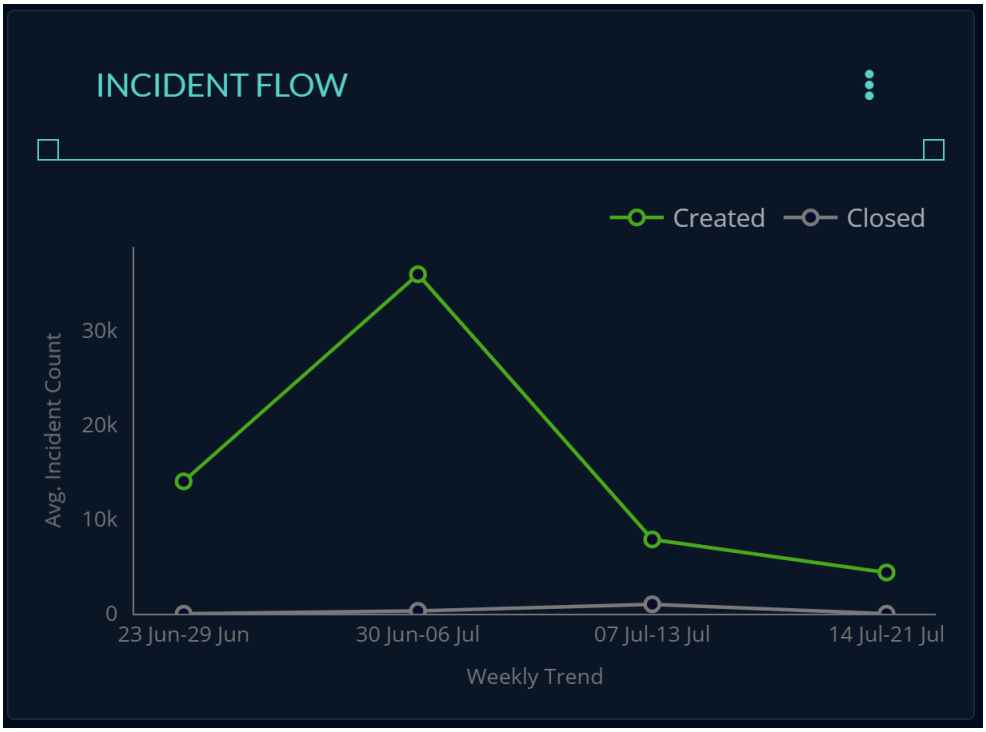
2. Configure the following options based on your preference:
   - **Time Range**: This option sets the date range. Options include Last 30 Days or Last 90 Days.
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

Incident Flow

This widget provides information about the average number of incidents that are closed among the total number of incidents created in respond. It enables the Managers to effectively analyze and process the ratio between the incidents created vs closed which gives an insight of why a segment of the workflow is trending differently.

A line graph visually presents the dataset. By default, it showcases the values for created and closed critical incidents over a time range of 30 days on a weekly trend. However, users have the option to set the global time filters to display the data for a maximum of 90 days. Each line segment in the chart is color-coded to represent a specific incident, as indicated by the chart legend.

The vertical axis shows the average incident count, while the horizontal axis shows the weekly trend.

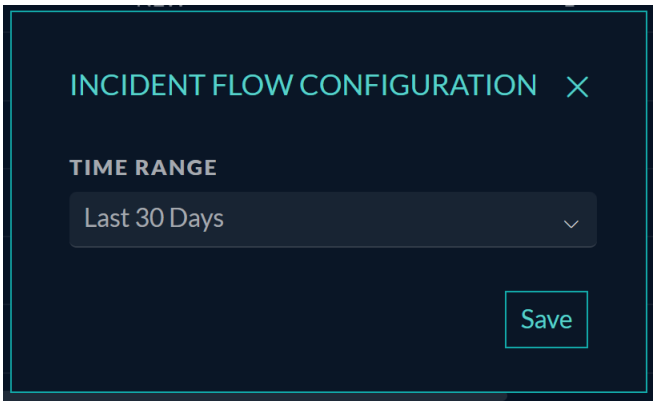


Placing the cursor over a graph line will display a tooltip allowing the user to view the exact values of average incident count for each created, open and closed incidents represented in that displayed week.

To edit the Incident Flow widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.

   The **Incident Flow Configuration** dialog is displayed.

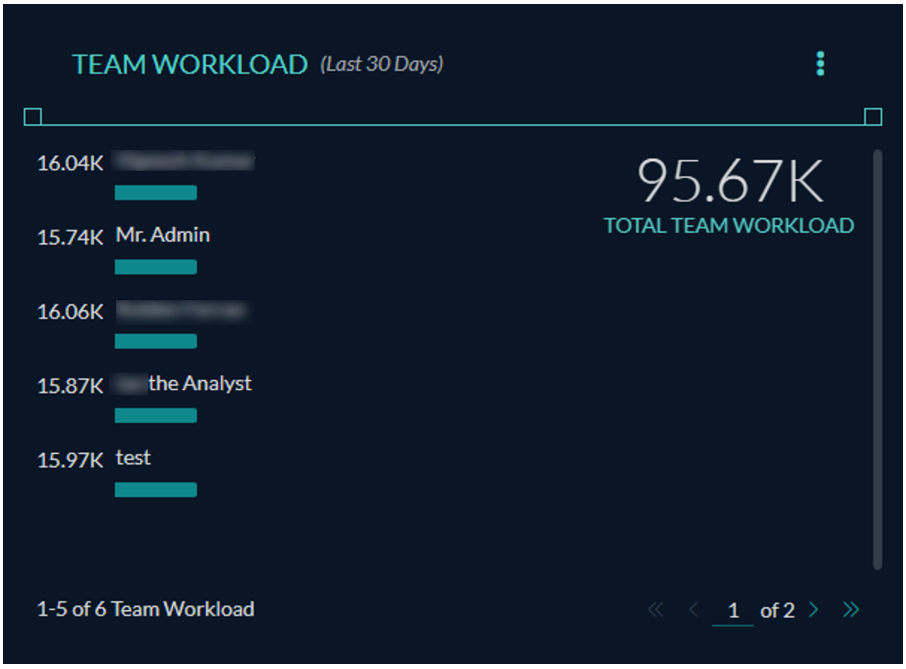


2. Configure the following options based on your preference:
   - **Time Range**: This option sets the date range. Options include Last 30 Days or Last 90 Days.
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

Team Workload

This widget displays the total number of incidents handled by each assignee in the team for the selected time range. The widget also displays the total team workload of all the incidents associated with each assignee in the team. It enables the Managers to view the team's performance and equally distribute the work among different team members.

A stacked bar graph visually presents the dataset. By default, it showcases the number of incidents handled by each assignee for the last 30 days. However, users have the option to configure the widget to display the data for a maximum of 90 days. The selected time range is displayed in front of the widget name. Each bar segment displays the assignee name and total incidents handled. Users also have the option to configure the number of results.

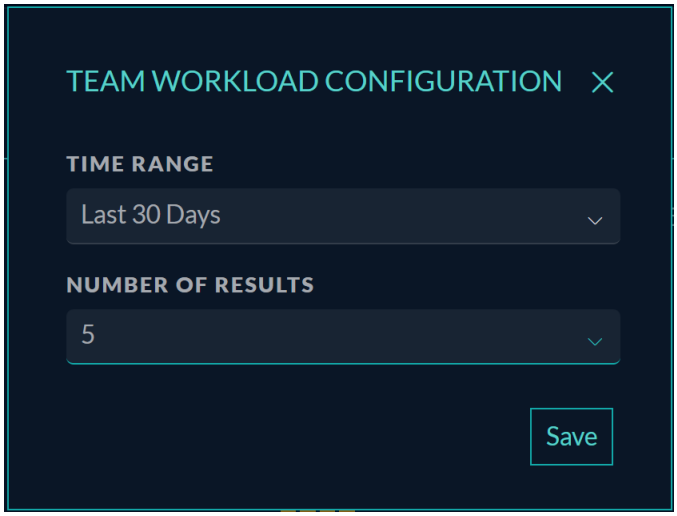


Placing the cursor over a graph bar will display a tooltip allowing the user to view the exact values of incidents handled by the selected assignee.

To edit the Team Workload widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.

   The **Team Workload Configuration** dialog is displayed.



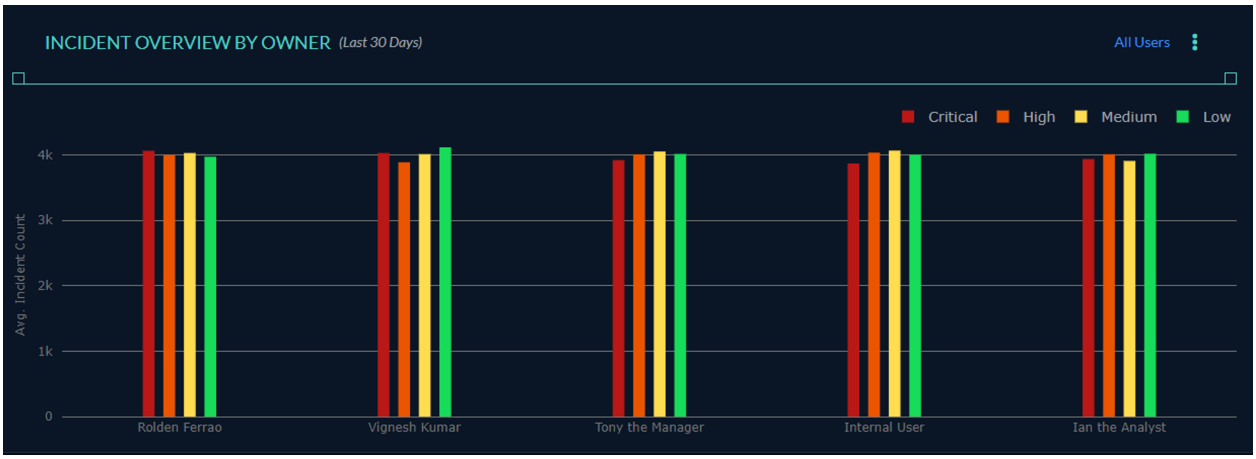
2. Configure the following options based on your preference:
   - **Time Range**: This option sets the date range. Options include Last 24 hours, Last 7 Days, Last 30 Days or Last 90 Days.
   - **Number of Results**: This option sets the number of results to be displayed on the widget.
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

Incident Overview by Owner

This widget displays the number of Critical, High, Medium, and Low priority incidents handled by each assignee in the team for the selected time range. The widget also displays the total incidents based on priority associated with each assignee in the team. It enables the Managers to view the number of incidents by priority.

A stacked bar graph visually presents the dataset. By default, it showcases the number of incidents based on the selected priority handled by each assignee for the last 30 days. However, users have the option to configure the widget to display the data for a maximum of 90 days. The selected time range is displayed in front of the widget name. Each bar segment in the chart is color-coded to represent the incident priority, as indicated by the chart legend.

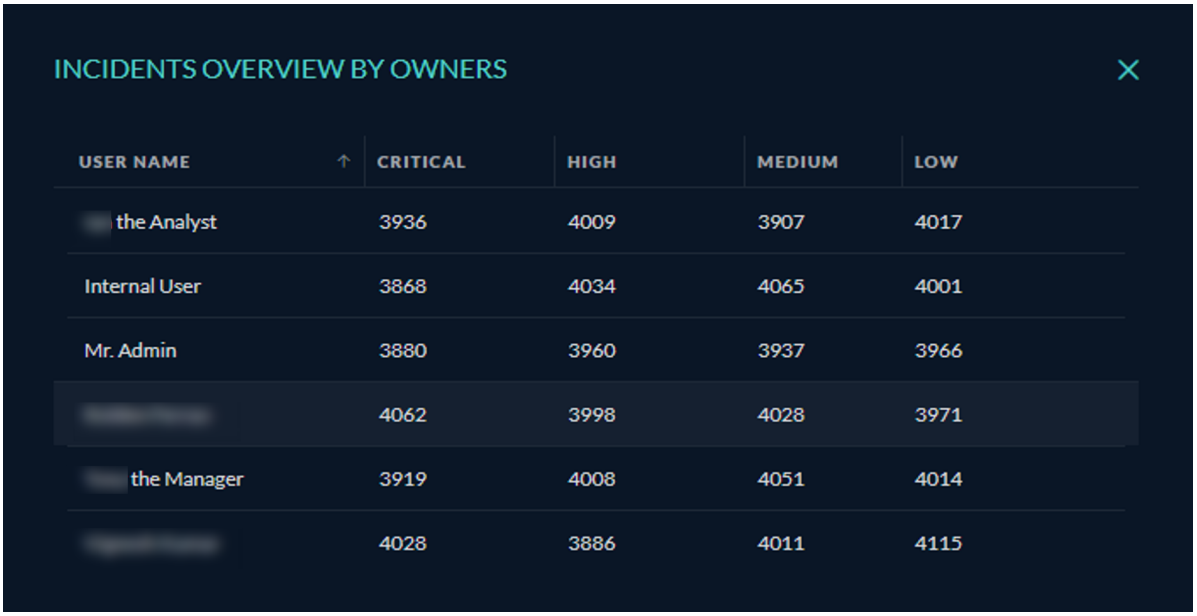
The vertical axis shows average incident count, while the horizontal axis shows the assignee with the selected priority. Users also have the option to configure the incident priority.



Placing the cursor over a graph bar will display a tooltip allowing the user to view the exact values of incidents based on the selected priority for the assignee.

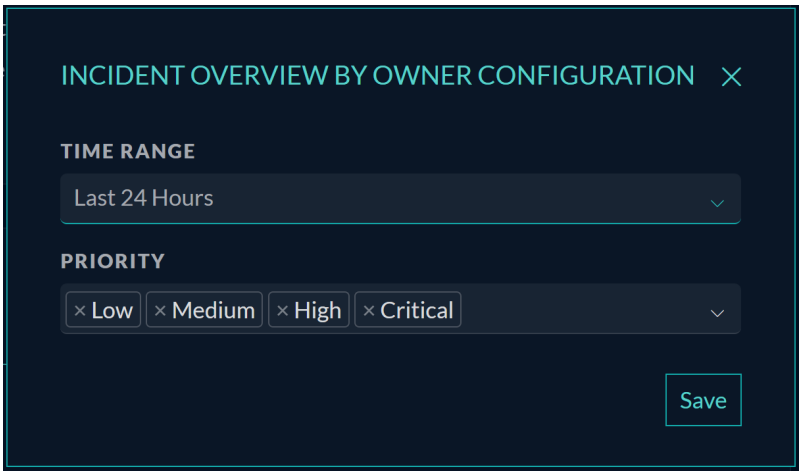
Note: This widget shows only the top 5 users in a graphical format.

Click **All Users** in the widget to view the numerical data of Critical, High, Medium, and Low priority incidents owned by each assignee in the team.



To edit the Incident Overview by Owner widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.
   The **Incident Overview by Owner Configuration** dialog is displayed.



2. Configure the following options based on your preference:
   - **Time Range**: This option sets the date range. Options include Last 24 hours, Last 7 Days, Last 30 Days or Last 90 Days.
   - **Priority**: This option sets the priority. Options include Low, Medium, High, and Critical.
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

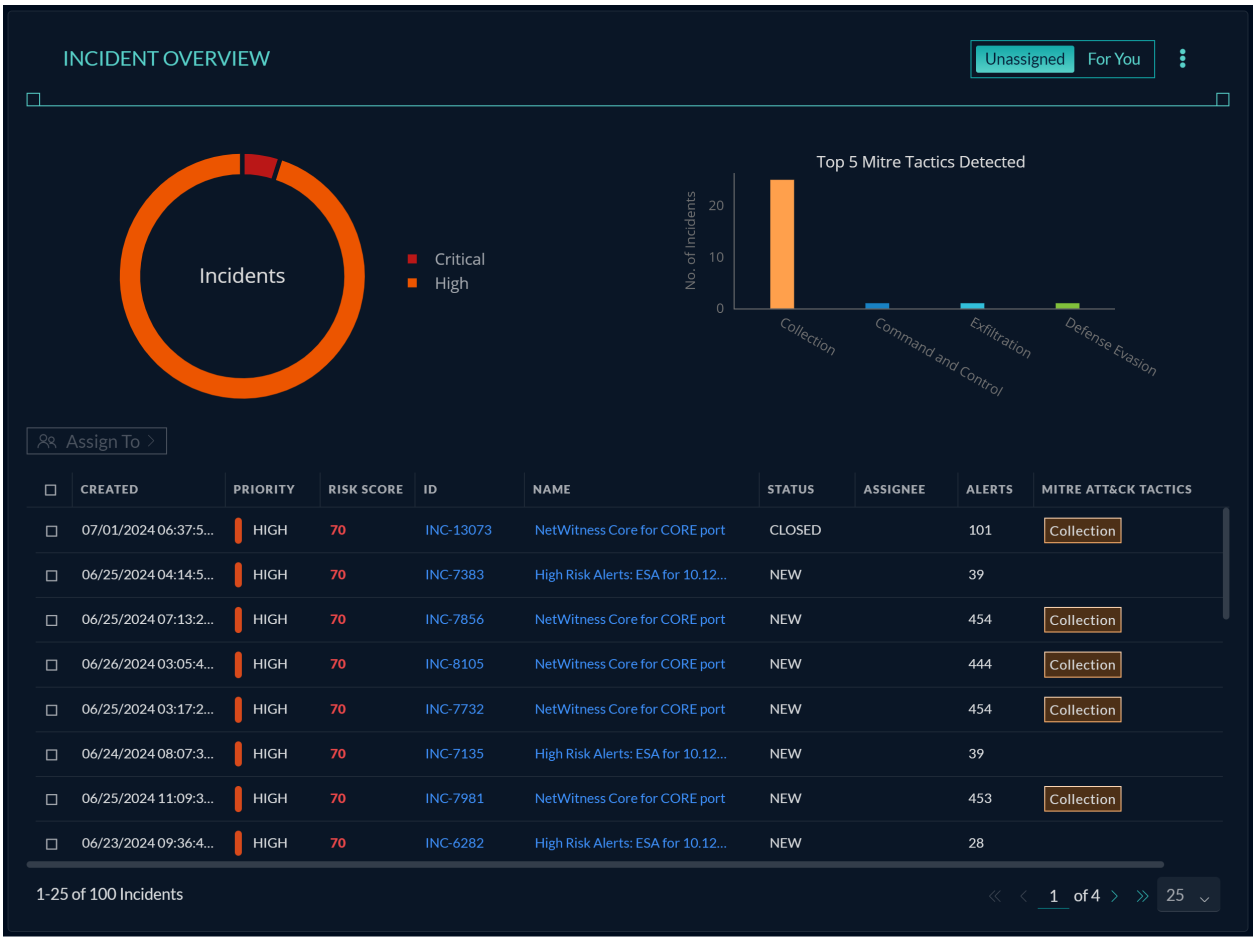
Incident Overview

This widget displays the following.

- List of all the unassigned incidents.
- List of all the incidents assigned to you.
- List of all the alerts (Users must edit the Configuration for the alerts to be displayed).

The incidents are listed in the columns Created, Priority, Risk Score, ID, Name, Status, Assignee, Alerts, and Mitre Att&ck Tactics. For more information on the columns displayed in the Incident Overview widget, see NetWitness Respond User Guide.

Note: By default, the widget displays the unassigned incidents. To view the incidents assigned to you, switch the toggle to **For You** in the widget.

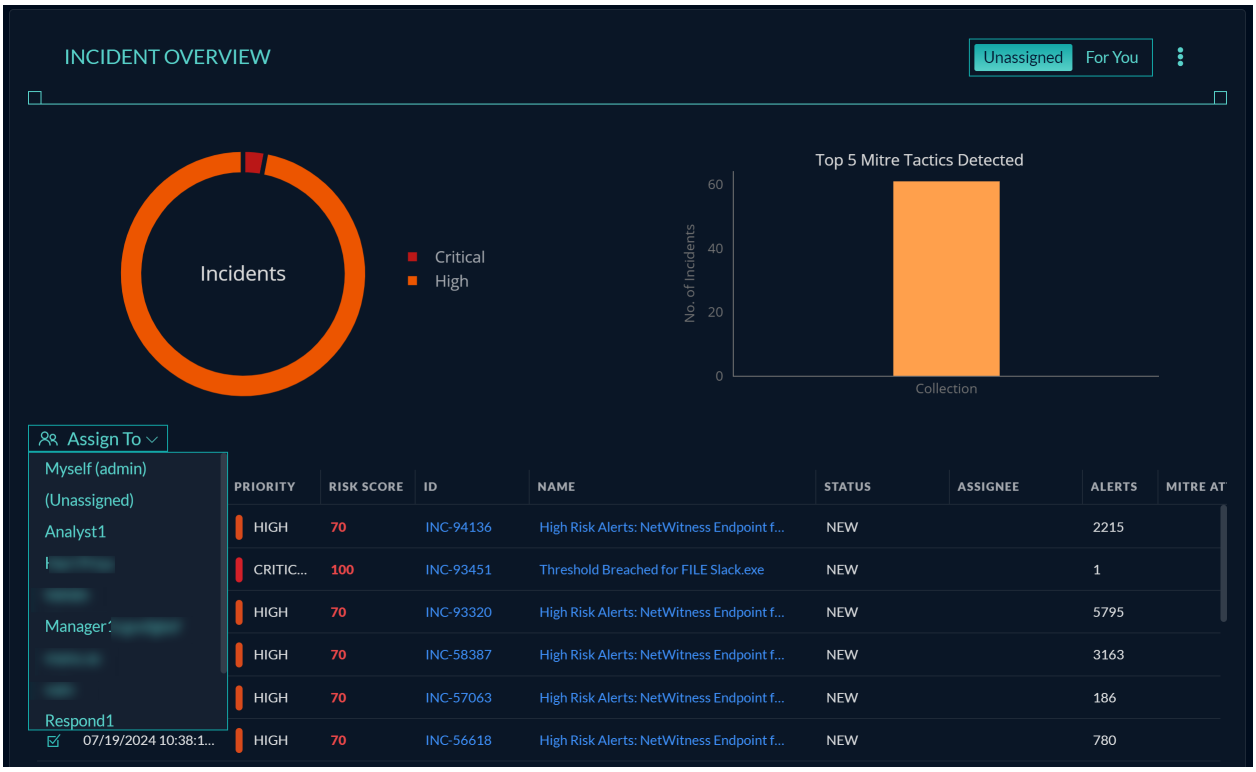


A color-coded donut chart at the top left displays the incidents based on the priority, as indicated by the chart legend.

A bar graph at the top right displays the Top 5 MITRE Tactics Detected. The vertical axis shows the number of incidents, while the horizontal axis shows the MITRE tactics.

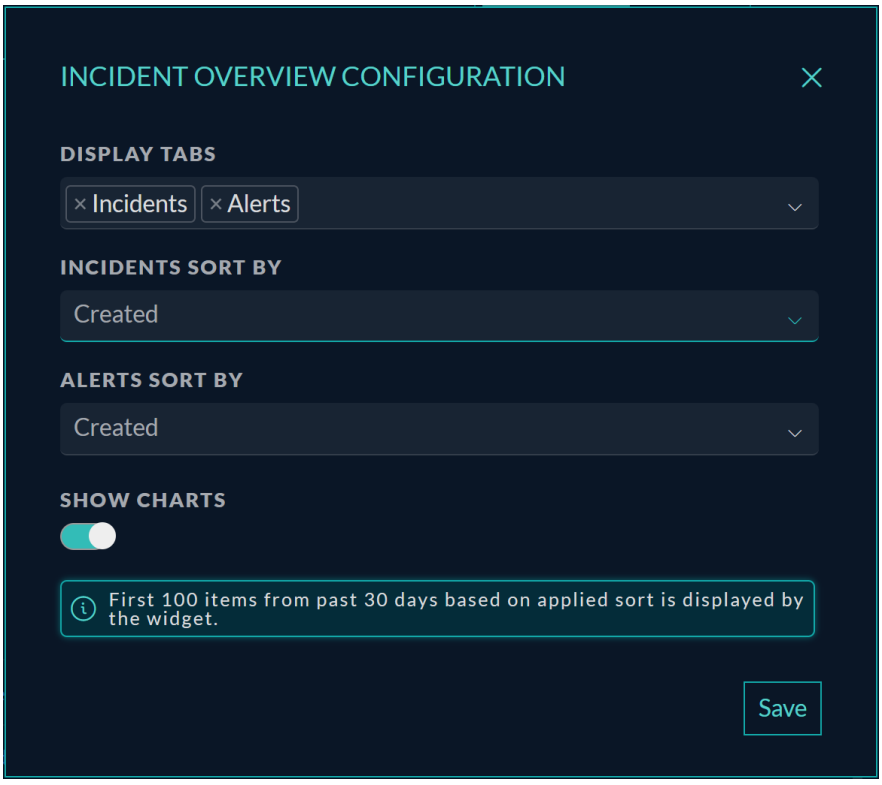
Placing the cursor over the donut chart and the bar graph bar will display a tooltip allowing the user to view the exact values of incidents.

Select any incident or incidents and click **Assign To**. A list of assignees is displayed to select and assign an incident.



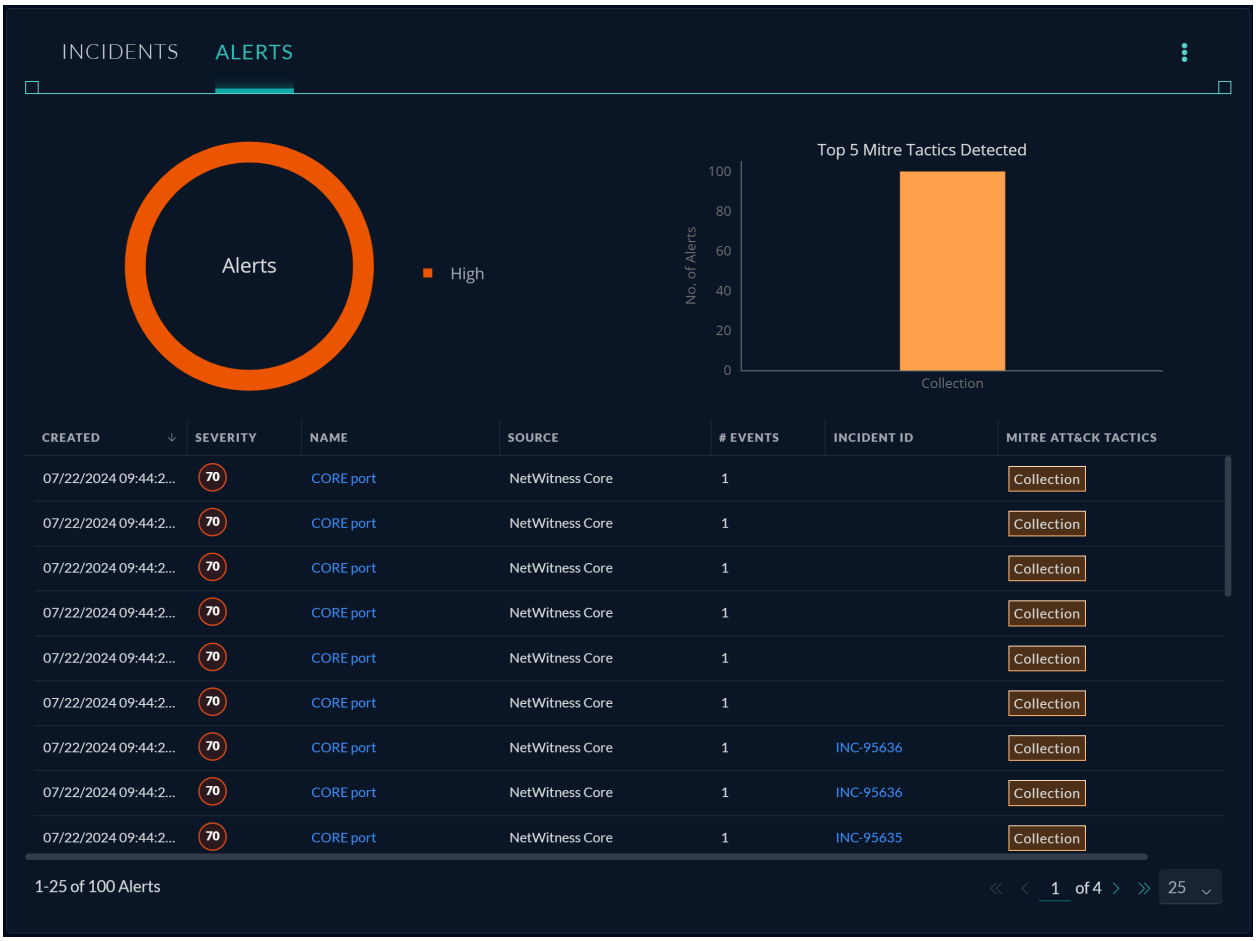
To edit the Incident Overview widget

1. Click the three-dot ( ) icon in the widget's upper-right corner and click **Configuration**.
   The **Incident Overview Configuration** dialog is displayed.



2. Configure the following options based on your preference:
   - **Display Tabs**: This option sets Incidents, Alerts or both on the Widget screen.
   - **Incidents Sort By**: This option sets the incidents sorting preference. Options include Created, Priority, Risk Score, Status, Assignee, and Alerts.
   - **Alerts Sort By**: This option sets the alerts sorting preference. Options include Created, Severity, Name, Source, and #Events.
   - **Show Charts**: This toggle option enables the display of charts in the widget screen.
3. Click **Save** to persist the changes made to the configuration.
4. Click **X** to close the Configuration dialog.

Note: On Selecting both Incidents and Alerts in the Display Tabs under Configuration, Users can view either a list of incidents or alerts on separate tabs.


INCIDENTS
ALERTS
Alerts
High
Top 5 Mitre Tactics Detected
100
80
60
40
20
0
No. of Alerts
Collection
CREATED
SEVERITY
NAME
SOURCE
EVENTS
INCIDENT ID
MITRE ATT&CK TACTICS
07/22/2024 09:44:2...
70
CORE port
NetWitness Core
1
INC-95636
INC-95635
Collection
1-25 of 100 Alerts
1 of 4
25

Error Messages for Widgets

This topic provides an overview of various configuration and access issues encountered in NetWitness Widgets on the Home page, along with corresponding recommended actions.

Following is a list of error codes displayed on the widget screen. Please reference the error code number when contacting support for assistance.

Error Codes	Title	Description
1101	Widget Data Retrieve Error	An unexpected error has occurred attempting to retrieve this data. Try again later.
1102	Live Account Unavailable	Either live account is not configured or there is an issue connecting to the live server. Configure live and try again or contact your administrator.
1301	Respond Server not configured	Please configure Respond server. For more details contact your administrator.
1302	Respond Server offline	The Respond Server is not running or is inaccessible. For more details contact your administrator.
1303	Access is denied	You do not have the required permissions to view Respond content. For more details contact your administrator.
1304	SLA not configured	Please configure the SLA in widget configuration. For more details contact your administrator.
1401	Access is denied	You do not have the required permissions to view Investigate content. For more details contact your administrator.
1402	Investigate Server is offline	The Investigate Server is not running or is inaccessible. For more details contact your administrator.
1501	Access is denied	You do not have the required permissions to view Endpoint content. For more details contact your administrator.
1502	Endpoint Server not configured	Please configure Endpoint server. For more details contact your administrator.
1503	Endpoint Server is offline	The Endpoint Server is not running or is inaccessible. For more details contact your administrator.
1601	Access is denied	You do not have the required permissions to view UEBA content. For more details contact your administrator.
1602	UEBA Server not configured	Please configure UEBA server. For more details contact your administrator.
1701	Access is denied	You do not have the required permissions to view Cloud Connector content. For more details contact your administrator.

Error Codes	Title	Description
1702	Cloud Connector Server not configured	Please configure Cloud Connector server. For more details contact your administrator.
1703	Cloud Connector Server is offline	The Cloud Connector Server is not running or is inaccessible. For more details contact your administrator.
1801	Source Server Offline	The Source Server is not running or is inaccessible. For more details contact your administrator.
1802	Source Server Data Retrieve Error	An unexpected error has occurred attempting to retrieve this data. Try again later.
9999	Unhandled Error	An unhandled error has occurred. For more details contact your administrator.

Note: If you encounter any error codes not listed above, review the service health and configuration settings. If the service is offline, try restarting it. If the problem persists, reach out to Customer Support for assistance.

Managing the Springboard

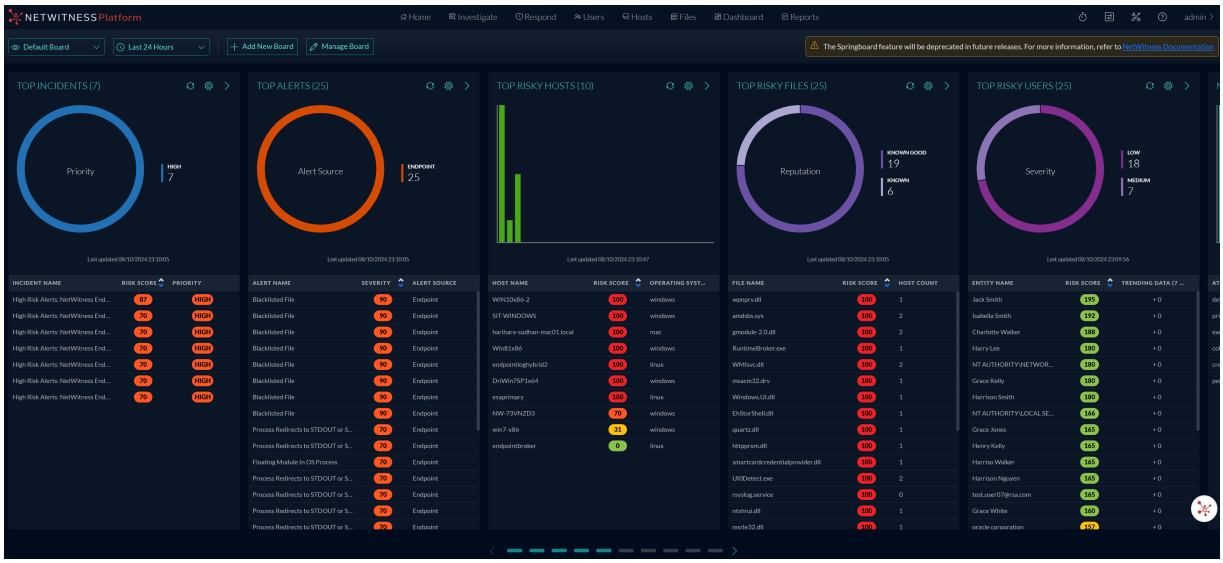
NetWitness Platform Springboard presents platform-wide detections and signals in this view so analysts hunt and investigate faster than ever before.

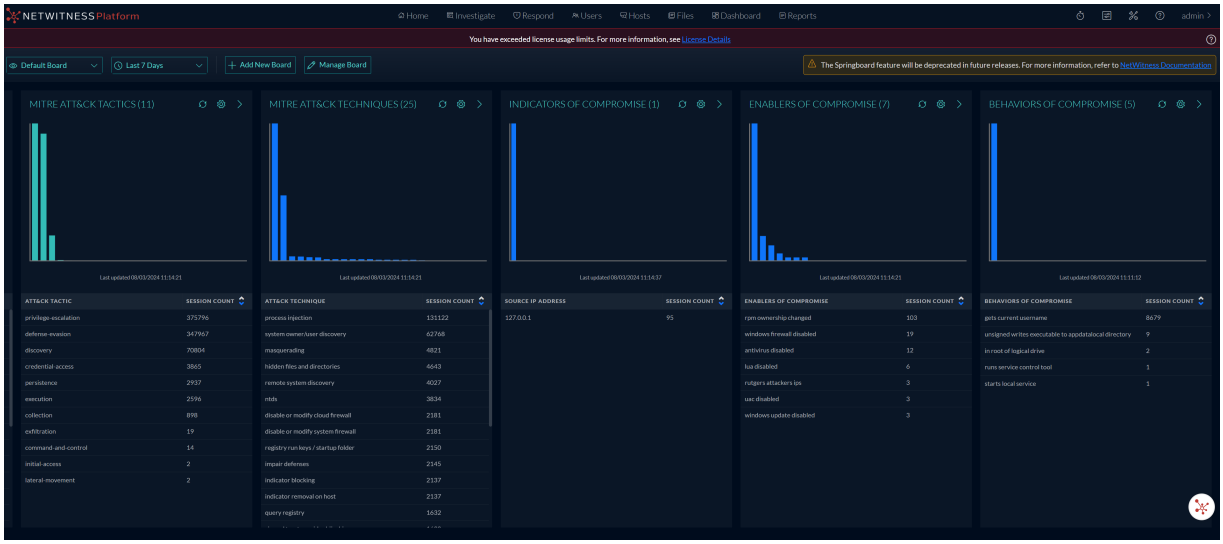
NetWitness consists of 10 out-of-the-box panels based on the data processed and presented on Springboard view. This helps analysts with further investigation.

Note: From NetWitness 12.5 and later, the **Home** page will be the default landing page for users installing the NetWitness Platform for the first time. For existing users, Springboard will still be the default landing page. However, the Springboard feature will be deprecated in future releases, and the Home page will become the default landing page. Users can click the **Home** page to view the new widgets.
All the information in the Springboard panels will be available on the new Home page, but users cannot migrate the data from the Springboard panels to the new Home page widgets. Also, users can change the default landing page using the **User Preferences > Default Landing Page** option. For more information, see the topic Setting User Preferences.

The Springboard congregates the following information for analysts to view:

- Critical incidents and high severity alerts that require attention.
- Hosts and files with high risk scores that may be potential threats.
- Risky users that are potential leads for investigation.
- Events with specific query and high severity that require immediate attention.





The Springboard displays important information for the last 24 hours in the following out-of-the-box panels:

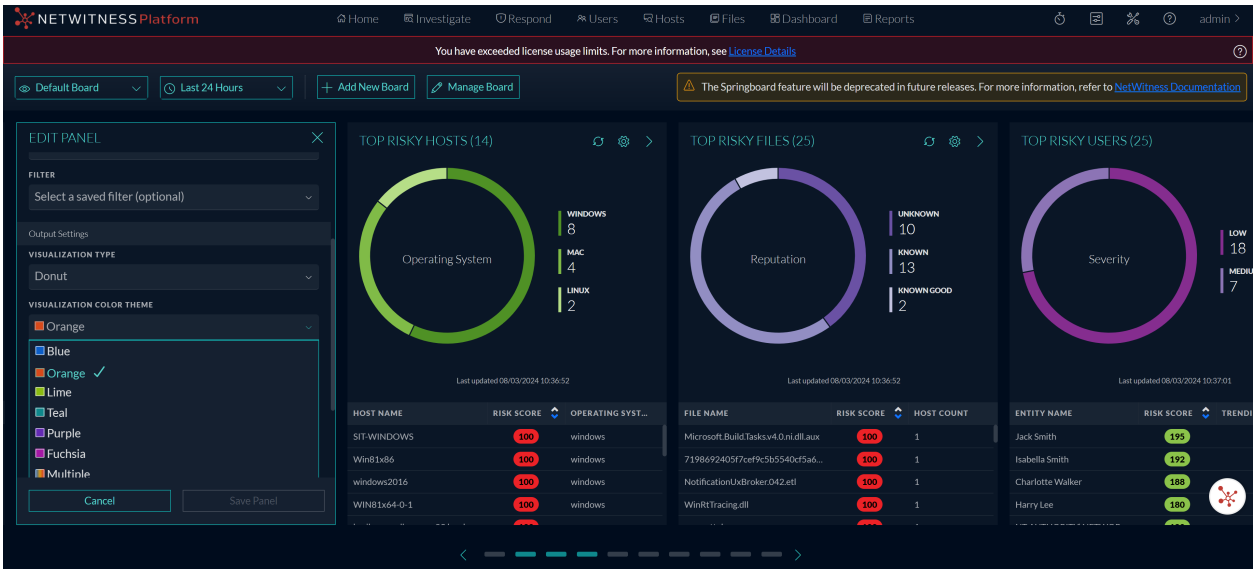
- **Top Incidents**
- **Top Alerts**
- **Top Risky Hosts**
- **Top Risky Files**
- **Top Risky Users**
- **MITRE ATT&CK tactics**
- **MITRE ATT&CK techniques**
- **Indicators of Compromise**

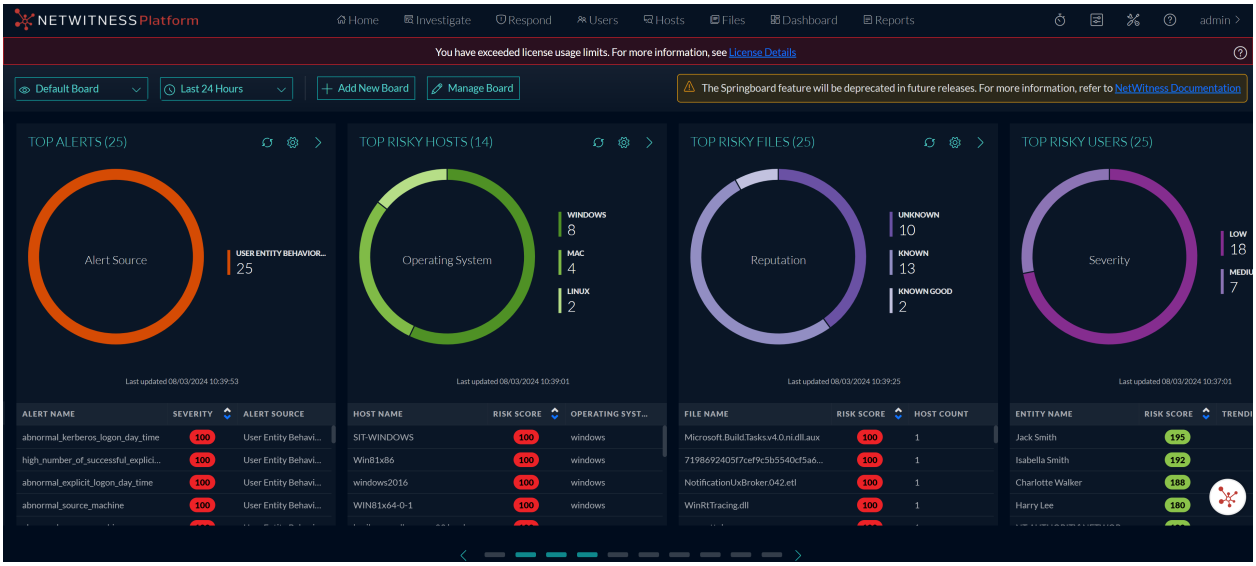
- **Enablers of Compromise**
- **Behaviors of Compromise**

For example, the Top Risky Hosts displays the top 25 risky hosts based on the highest risk score and Operating system (Windows, Linux, and Mac). The result displays hosts of all Endpoint Servers if the Endpoint Broker is available. Otherwise, it displays the result of the first Endpoint Server.

NetWitness Springboard provides the ability for analysts to choose from a variety of color palettes when creating or editing panels using the **Visualization Color Theme** option. This option gives analysts more control over the appearance of their panels, making them more visually appealing and easier to understand. As a result, analysts can visualize the data better and perform analysis and investigations more efficiently.

Note: The **Multiple** color option is available only for the Donut chart.





You can perform the following actions on the Springboard:

- Change the time range for some panels namely Incidents and Alerts panels. To change the time range, select the time range selection box from the drop-down menu in the top left corner of the Springboard view.

  IMPORTANT: If the selected filter has a time range selected, it is given priority, otherwise the Springboard time range for the specified panel is considered.

- Increase the display of the results in the table to view more than 25 results. Click on the panel, the Edit Panel dialog is displayed. Edit the number of results field and click **Save Panel**.
- Click a row in the table to view details or to investigate.
- Click at the top of the panel to view all the results. For example, in the Top Incidents panel, click to view all incidents in the **Incidents** list view.
- Click a row name in the events panel to view or investigate the event details with relevant filters applied in the **Events** view.
- Scroll to view the different panels using the scroll bar available below the panels.

Administrators can customize the Springboard by performing the following:

- Create own custom private board and add panels on the board. For more information, see Add a Custom Private Board.
- Edit the out-of-the-box panels. For more information, see Edit a Panel.
- Refresh the out-of-the-box panels. For more information, see Refresh a Panel.
- Create new panels with important system indicators. For example, a new panel showing focused event metadata based on pre-defined query conditions can be created. For more information, see Add a Panel.

Working with the Springboard

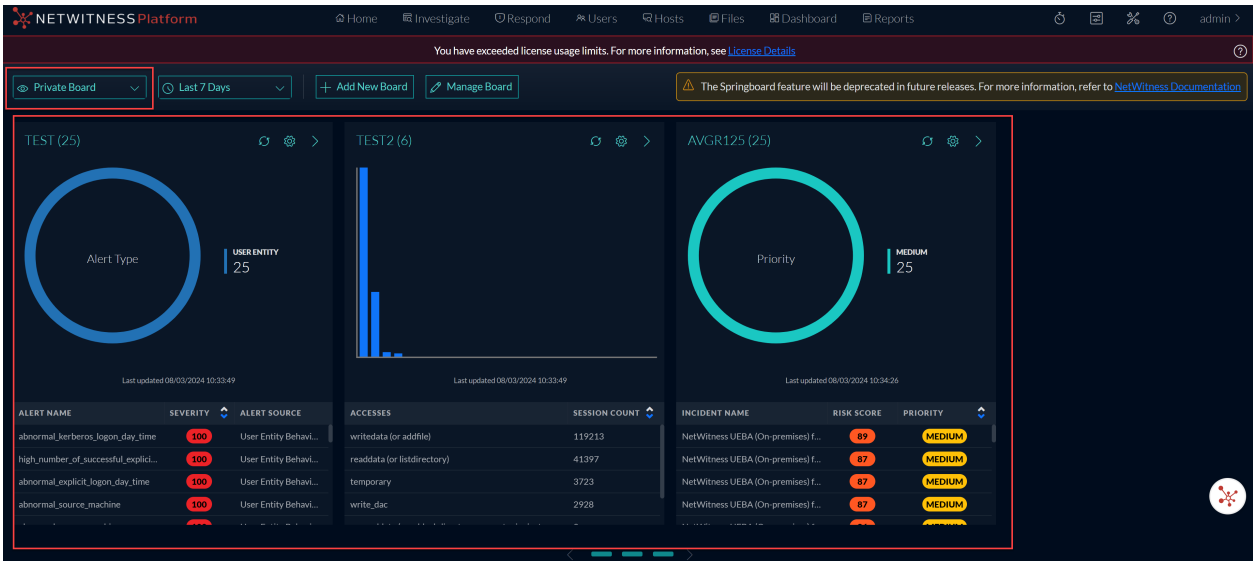
Note: An administrator must provide the appropriate permissions to allow users to edit the springboard panels. For more information see the the Springboard section in the "Role Permissions" topic in the *System Security and User Management Guide.*

You can customize the information on the out-of-the-box Springboard by adding, editing, copying, moving, and deleting panels.

The data sources and query filters are automatically added for the out-of-the-box panels.

Add a Custom Private Board

Administrators and Analysts can create their own custom private board in the springboard and add panels with important system indicators, which helps in threat hunting and investigation. The users can also add, edit, rearrange, and delete panels in the custom private board view. The board allows users to organize and manage information in an easy manner.

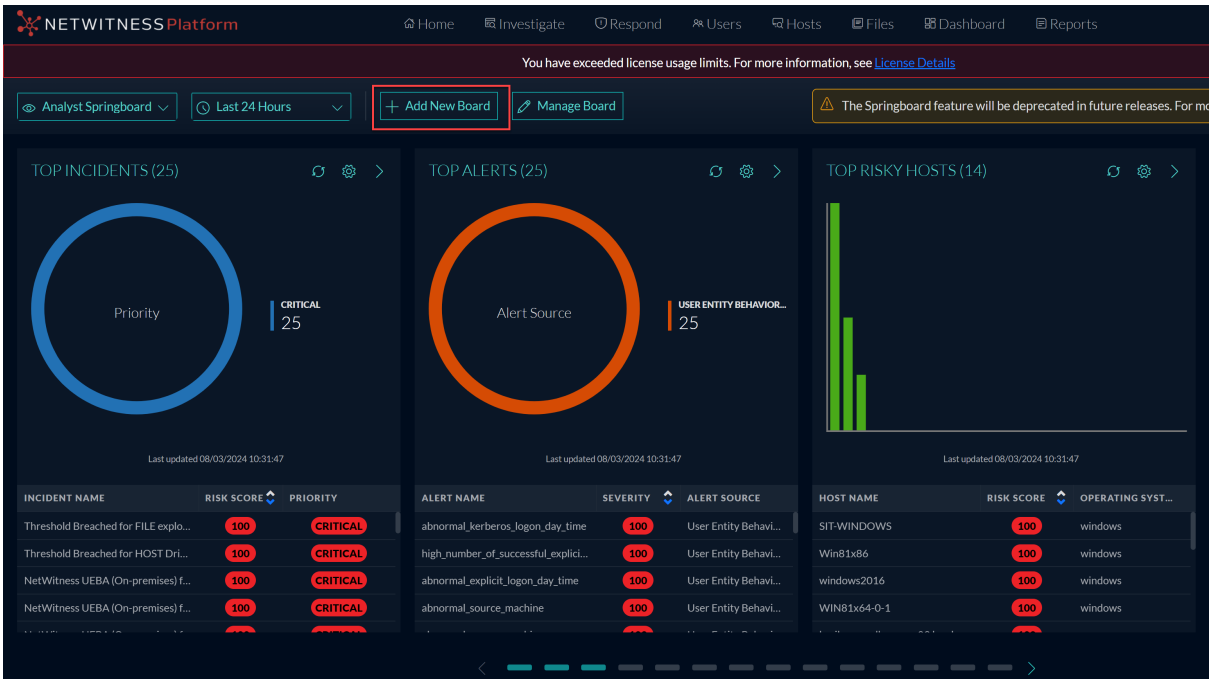


IMPORTANT:
- The board will be saved as a custom private board, and other users will not be able to view the board.
- Only one custom private board can be created.

Note: The maximum number of panels on the custom private board must not exceed 20 panels.

To add a custom Board:

1. Click + **Add New Board**.



   It navigates to a custom private board view to add panels.

2. Add the panels. For more information, see Add a Panel.

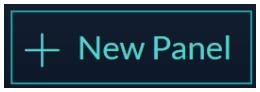
3. To edit the custom board's name, click at the top left corner and enter a unique name.
4. Click **Save Board**.

Add a Panel

You can add a panel to the Springboard according to the analyst preferences. For example, an analyst can watch top risky users or top risky hosts for a particular region in a panel.

Note: The maximum number of panels on the Springboard should not exceed 20 panels.

To add a panel:

1. Click **Manage Board**.
2. Click 

either on the top or on the right side of the view or click  at the bottom of the view to add a panel.

   The Create New Panel dialog is displayed. The following figure is an example of the events panel

configuration.

3. In the Input Settings section:
   - **Name**: Enter a unique name for the panel. The name can include letters, numbers, spaces, and special characters, such as `_ - ( ) [ ]`.
   - **Number of Results**: By default, the number of results is 25. Specify the number of results that range from 25 to 100.
   - **Data Type**: Select the type of data to use for the panel:
     - Alerts
     - Incidents
     - Events
     - Files
     - Hosts
     - Users
     - Assets
   - **Data Source**: Select the source of the data to use for the panel. This field is enabled when the data type is Events, Files, Hosts and Users.
     - Events: Select either Broker or Concentrator.
     - Files: Select either Endpoint Broker Server or Endpoint Server.
     - Hosts: Select either Endpoint Broker Server or Endpoint Server.
     - Users: Select either UEBA Server 1 or UEBA Server 2.

       Note: You can only select different data sources for **Users** if you have configured multiple UEBA servers in your environment. For more information, see "Configure Multiple UEBA Servers" in *NetWitness UEBA Configuration Guide*.
   - (Optional) **Filter**: Filter the data as required from the drop-down for each data type from the saved filters list.
4. In the Output Settings section, select the appropriate settings based on the data type.
5. Click **Add Panel**.
6. Click **Save Board** once you have added all the panels.

Edit a Panel

You can edit the out-of-the-box or newly added panels on the Springboard.

To edit a panel:

1. Click on the panel that you want to edit.
   The Edit Panel dialog is displayed.
2. Edit and click **Save Panel**.

Rearrange Panels

You can arrange the panels by dragging and dropping them into a different order on the Springboard.

To rearrange panels:

1. Click **Manage Board**.
2. To move a panel, click anywhere on the panel, drag and drop the panel to the desired location.
3. Click **Save Board**.

Delete Panels

You can delete panels permanently in the following situations:

- Services are not installed. For example, if you do not have Endpoint Log Hybrid installed, then you can delete the panels for Top Risky Hosts and Files.
- The maximum number of panels have exceeded the limit, that is 20, and you want to add a new panel.

To delete existing panels:

1. Click **Manage Board**.
2. Select the panels that you want to delete.
3. Click **Remove Panel**.
4. Click **Save Board**.

Restore System Default Settings

Note: This is enabled only if any changes are made to the out-of-the-box Springboard panels.

To restore the out-of-the-box panels:

1. Click **Manage Board**.
2. Click **Restore System Default**.

A confirmation pop-up is displayed to confirm if you want to restore the out-of-the-box panels or not.

3. Click **Restore System Default**.

Refresh a Panel

To refresh a panel:

Click  on the panel that you want to refresh, it loads the latest data in the panel.

Managing Dashboards

A dashboard is a group of dashlets that give you the ability to view data in one space, the key snapshots of the various components that you consider important. In NetWitness, you can compose dashboards to obtain high-level information and metrics that portray the overall picture of a NetWitness deployment, displaying only the information that is most relevant to the day-to-day operations.

The dashboards for all NetWitness components are available to add to the default NetWitness dashboard or a custom NetWitness dashboard.

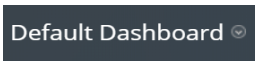
You can view dashboards on different areas of interest depending on your user permissions. You have the option to select a preconfigured dashboard, import a dashboard, or create your own custom dashboard. The dashboards help you to quickly and easily view reports. You can configure your dashboards to display the information that supports your workflow. This topic explains the high-level tasks that can be done when you are setting up a dashboard.

Dashboard Basics

If the Dashboard view is your default landing page following logging in to NetWitness, you always see either the default dashboard or the currently configured dashboard immediately after completing the login process. To return to the dashboard from another NetWitness component, click **Dashboard**.

Dashboard Title

The dashboard title reflects the currently active dashboard; for example, Default Dashboard.



Dashboard Selection List

You can access preconfigured and custom dashboards on the dashboard selection list. When you select a dashboard, its title is displayed below the NetWitness toolbar.

A dashboard has:

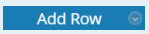
- The dashboard toolbar
- The dashboard title and the dashboard selection list.

Dashboard Toolbar

The dashboard toolbar is available next to the title of the selected dashboard. The dashboard toolbar allows various operations on dashboards and dashlets.

Note: The Copy, Delete, Import, Export, Share, and Add Row options are disabled for preconfigured dashboards.

Option	Description
★	Sets the selected dashboard as the Favorite.
Default Dashboard	Displays the list of available dashboards from which you can make a selection.

Option	Description
	Displays the Create a Dashboard dialog, where you define or add a custom dashboard.
	Deletes a custom dashboard. The default dashboard cannot be deleted.
	Allows you to copy a dashboard.
	Displays the Manage Dashlet dialog.
	Exports a dashboard as a .zip file.
	Imports a dashboard as .zip or.cfg file.
	Allows you to share a dashboard with another user.
	Enables user to add rows and columns to the dashboard based on the requirement. Click the  icon in a row to add a dashlet.

The Default Dashboard

The default dashboard is configured to display specific dashlets in specific positions. The default dashboard serves as an example of dashboard composition and a starting point for customization.

- You can customize the information on the default dashboard by editing, adding, moving, maximizing, and deleting dashlets.
- After modifying the default dashboard, you can restore the default dashboard () to its original layout.
- The default dashboard cannot be deleted or shared.

Selecting a Preconfigured Dashboard

On installation of NetWitness, the following preconfigured dashboards are automatically activated and are available to you:

- Default
- Identity
- Investigation
- Operations - File
- Operations - Logs
- Operations - Network
- Operations - Protocol Analysis
- Overview
- RSA SecurID
- Threat - Hunting
- Threat - Intrusion
- Threat - Malware Indicators

You cannot perform the following actions on a preconfigured dashboard:

- Edit a dashboard
- Export a dashboard
- Share a dashboard
- Delete a dashboard

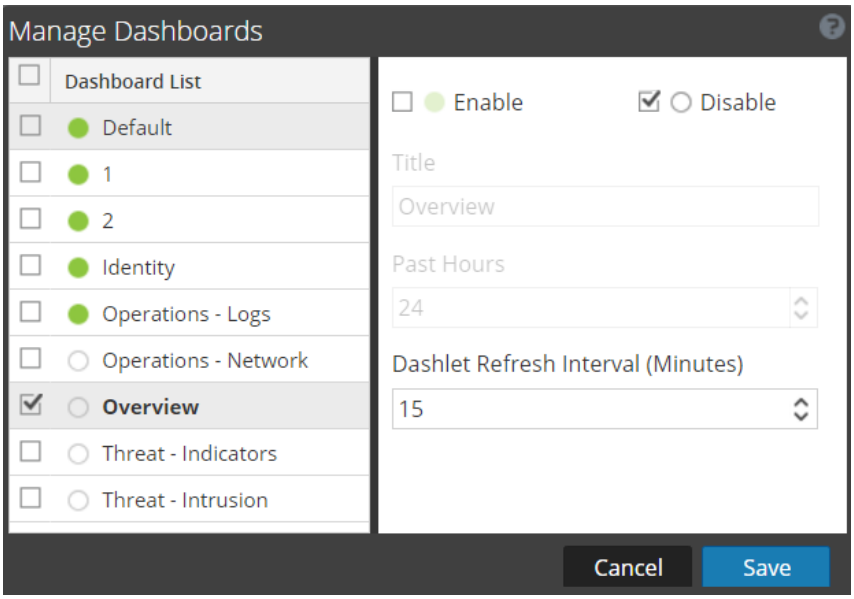
For more information on each preconfigured dashboard, see the Dashboards Catalog in the NetWitness Content space on NetWitness Community.

Note: If you are logged into an Analyst UI, you can view but cannot enable, disable, or edit preconfigured Dashboards.

Enabling or Disabling Dashboards

When you enable or disable a dashboard, all the dashlets within the dashboard are enabled or disabled along with the associated charts, unless they are used in any other dashboard.

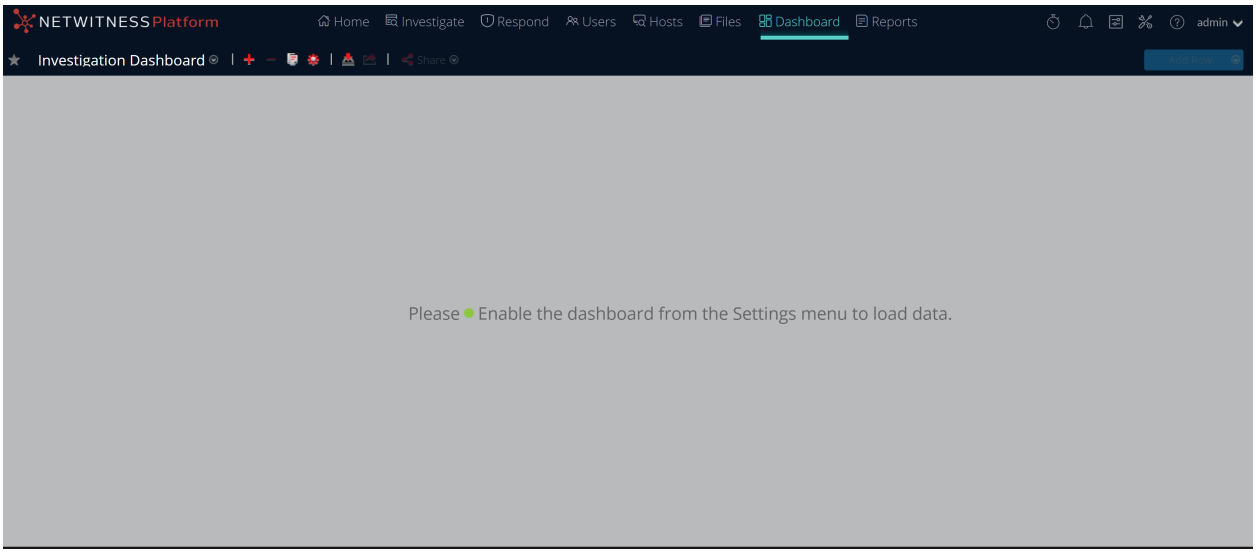
NetWitness modules can display only those dashlets presented in the Manage Dashboard dialog. The main dashboard offers all NetWitness dashlets. This is an example of currently available dashlets.



Name	Description
Dashboard List	Displays a list of the default, preconfigured, and custom dashboards.
Enable	Indicates if the selected dashlet is enabled.
Disable	Indicates if the selected dashlet is disabled.
Title	Displays the title of the selected dashlet and you can also rename the dashboard.
Past Hours	Displays the time for which the data is collected.
Dashlet Refresh Intervals (Minutes)	Displays the refresh interval time of a dashlet.

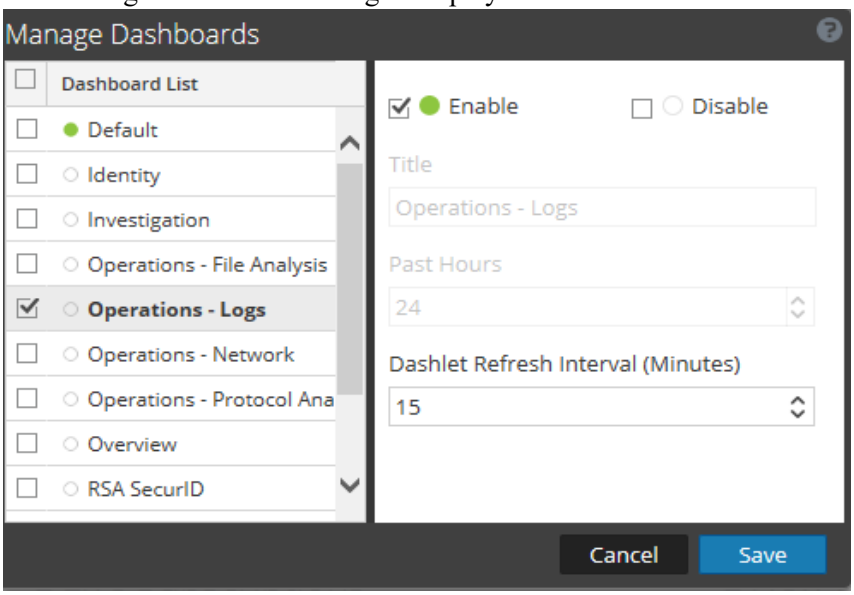
Enable a Dashboard

If you select a dashboard that is not enabled, a masked screen is displayed.



To enable one or more dashboards:

1. Navigate to the dashboard to be enabled.
2. In the dashboard toolbar, click  (Manage Dashboards).
   The Manage Dashboards dialog is displayed.

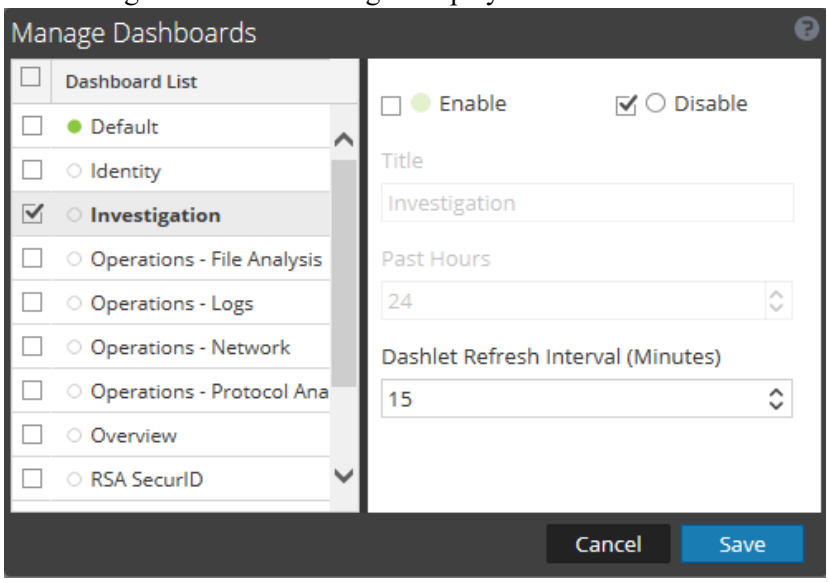


3. From the dashboard list, select the dashboards to be enabled.
4. Select the **Enable** checkbox.
5. Click **Save**.

Disable a Dashboard

To disable one or more dashboards:

1. Navigate to the dashboard to be disabled.
2. In the dashboard toolbar, click  (Manage Dashboards).
   The Manage Dashboards dialog is displayed.



3. From the dashboard list, select the dashboards to be disabled.
4. Select the **Disable** checkbox.
5. Click **Save**.

Setting a Dashboard as a Favorite

To customize the views in NetWitness, you can set a preconfigured or custom dashboard as a Favorite. The NetWitness dashboard offers all NetWitness dashlets. The Favorite dialog sets a specific dashboard as your favorite dashboard and is listed as favorite every time you log in to NetWitness.

1. Navigate to any dashboard.
2. In the dashboard toolbar, click 

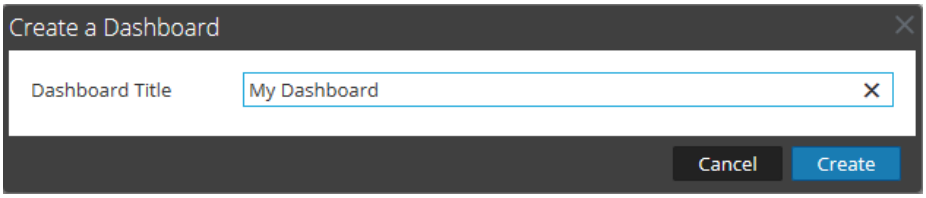
   If the favorite icon is red in color, it indicates that selected dashboard is set as a Favorite and is listed on top above the line.

Creating Custom Dashboards

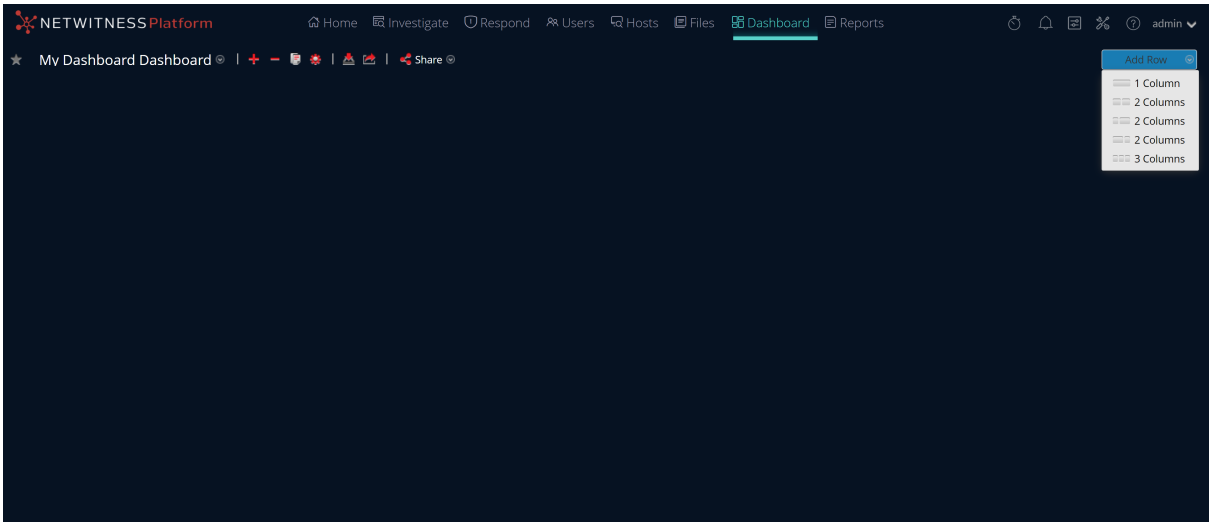
You can create custom dashboards to serve a particular purpose; for example, to represent a specific geographical or functional area of the network. Each custom dashboard is appended to the dashboard selection list.

To create a custom dashboard:

1. In the dashboard toolbar, click  .
   The Create a Dashboard dialog is displayed.



2. Enter a title for the new dashboard and click **Create**.
   The new dashboard is displayed as a blank screen.



3. Add rows to the dashboard, which can contain one or more columns, using the **Add Row** option on the right side of the screen (). Click the desired column configuration in the drop-down list to add one row to the dashboard with the selected number of columns. Repeat the process to add more rows.

4. You can add any desired dashlets to the dashboard by clicking  in an empty placeholder in a row. For complete details on adding and managing dashlets, see Working with Dashlets.

After custom dashboards are created, you can:

- Switch between dashboards by selecting an option from the dashboard selection list.
- Delete any custom dashboard.
- Import or export a dashboard.

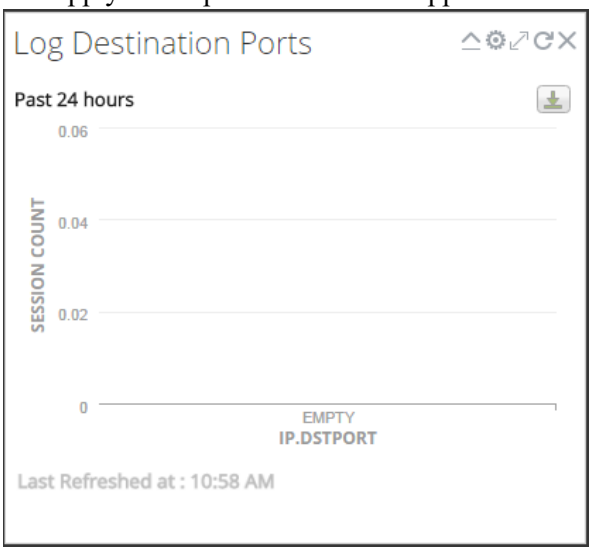
Each dashboard has:

- The dashboard toolbar.
- The dashboard title and the dashboard selection list.
- Zero or more dashlets.

Working with Dashlets

Dashlets are the parts that make up a dashboard. NetWitness uses dashlets to display focused subsets of system information, services, jobs, resources, subscriptions, rules, and other information.

The controls for a dashlet are in the title bar. All dashlets use a common set of controls, and only those that apply to the particular dashlet appear in the title bar of the dashlet.



The following table displays the description of each icon on the dashlet.

Icon	Name	Description
	Collapse vertically	Collapses the dashlet vertically so that only the title is visible.
	Expand vertically	Expands the dashlet to its original size.
	Reload	Reloads the dashlet.
	Settings	Displays configurable settings for the dashlet.
	Maximize	In some dashlets with content that does not fit horizontally within the width of the dashlet, maximizes a chart or a dashlet to full screen.
	Delete	Deletes the dashlet from the dashboard.
Last Refreshed at		Displays the time at which the data is polled from the related chart.

Icon	Name	Description
View More		When clicked, navigates to the corresponding dashboard which is linked to the main dashlet and displays more details. If you have not linked the dashboard to an existing dashlet, this link with not be available on the dashlet. To configure this option, click , and in the Dashboard Link field select a related dashboard view more details of the specific dashlet.

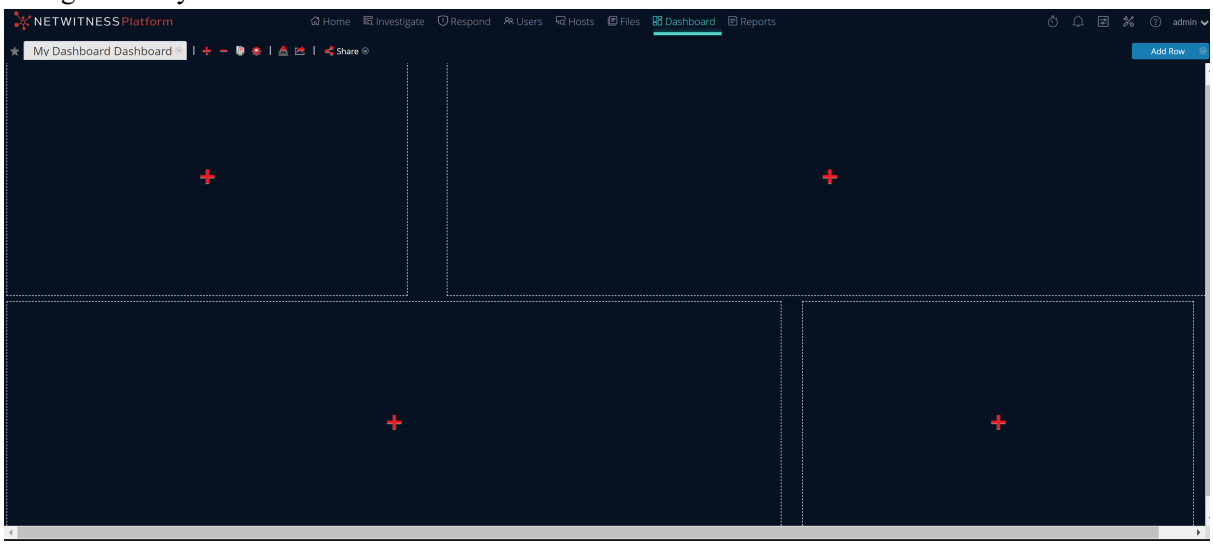
You can add dashlets to the default dashboard or construct a custom dashboard with your own useful set of dashlets to make your workflow more efficient.

Add a Dashlet

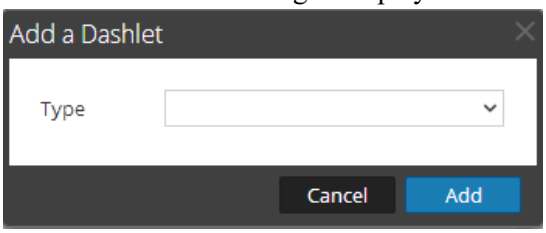
To customize the views in NetWitness, you can add dashlets to a default dashboard or create custom dashboards. However, you cannot add dashlets to preconfigured dashboards.

To add a dashlet:

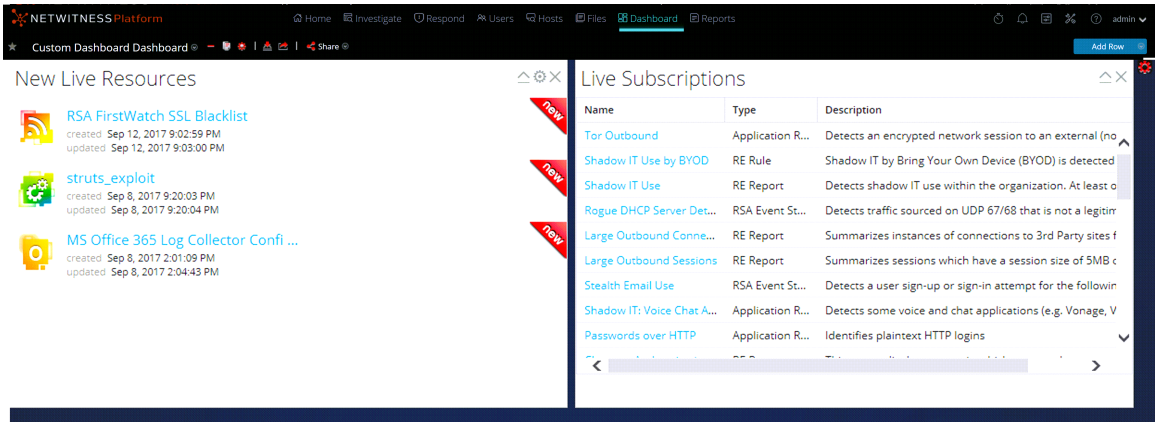
1. Navigate to any dashboard or create a new dashboard.



2. Click  on the placeholder where you want to add the dashlet.
   The Add a Dashlet dialog is displayed.



3. Click the **Type** selection list to view the available dashlets, and select the type of dashlet you want to add. Depending on the type of dashlet you are adding, some configurable fields appear in the **Add a Dashlet** dialog.
4. Type a title for the dashlet. The title can include letters, numbers, special characters, and spaces.
5. If there are additional configurable fields for the dashlet, set appropriate values.
6. When all required fields have been configured, click **Add**.
   The dashlet is added to the dashboard in the selected placeholder and is automatically saved.



Edit Dashlet Properties

All preconfigured dashlets are read-only and their properties cannot be edited. Other dashlets are editable and allow users to customize some aspect of the data displayed in the dashlet. A dashlet with editable properties has a settings (⚙) option that displays all the editing options.

After the dashlets are added, you can drag and drop them and they can be swapped.

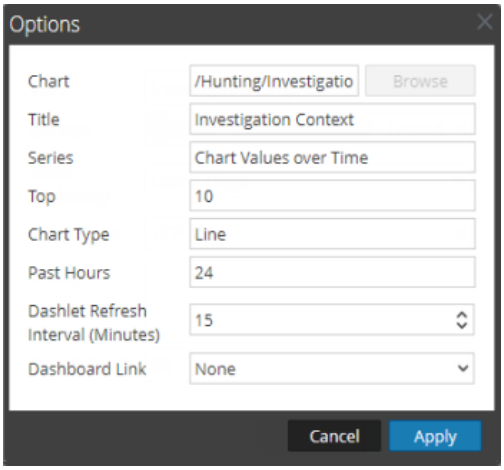
A dashlet without editable properties, such as the Live Subscriptions dashlet, does not display the settings option in the title bar. Many dashlets have an editable title where you can edit the following properties:

- Dashlet display title.
- Type of services to monitor; for example, you can monitor only Decoders, or you can monitor Decoders and Concentrators.

Other dashlets have parameters that you define to specify the kind and amount of information you want to see in the dashlet. For example, a Realtime Chart Dashlet has the settings option.

1. To display and modify the options for a dashlet, click settings ( ) in the dashlet title bar.

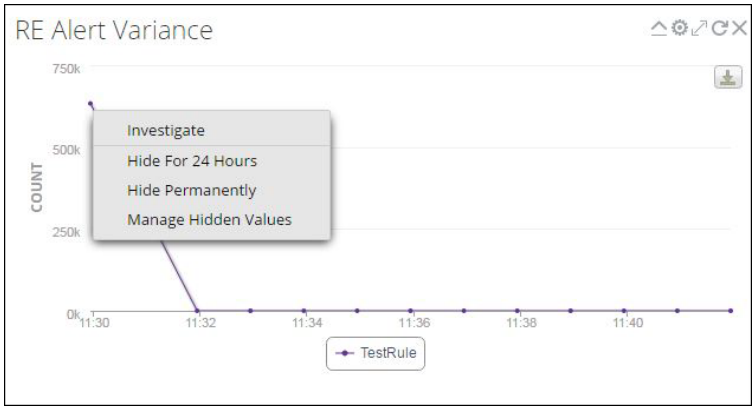
   The Options dialog is displayed.



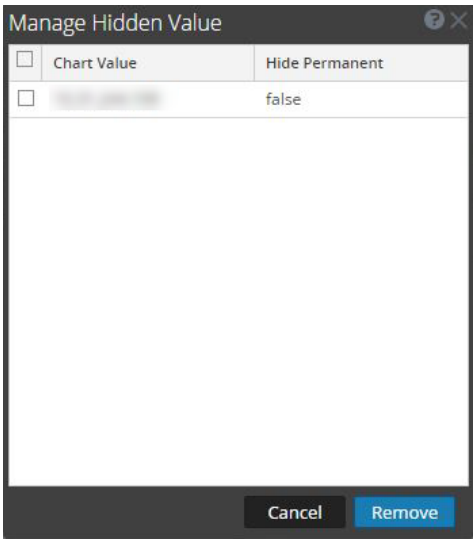
2. Edit any of the displayed properties. For example, in an in Operations - File Analysis Dashboard, edit Dashlet Refresh Interval from 15 to 20.
3. Click **Apply**.

Some dashlets have configuration options to tailor the appearance or the contents of the dashlet. The following options are available for RE Top Alerts, RE Alert Variance, and RE Realtime Charts dashlets on left-click:

- **Hide For 24 Hours**: This option allows you to hide the selected value for the next 24 hours. After 24 hours, the data is automatically displayed on the dashlet, if the value is configured and listed on top.
- **Hide Permanently**: This option allows you to hide the selected value permanently until you add it back using the Manage Hidden Values option.



- **Manage Hidden Values**: This option displays a list of all the hidden values. You can select the checkbox for a value and click **Remove** to view the data back on the chart.



The options to Hide for 24 Hours, Hide Permanently, and Manage Hidden Values are not available for Geomap charts.

Note: When you edit a value in a preconfigured dashboard, it is a user-specific change. The changes made to a preconfigured dashboard are applicable only to your dashboard and cannot be viewed by other users who use the same preconfigured dashboard. For example, if you hide a value in an overview dashboard, the change is applicable only to your dashboard. If another user views the same overview dashboard, the value is still displayed. The same applies to a custom dashboard. When you hide a value in the custom dashboard and share the same dashboard with another user, the values are still displayed even though the dashboard is shared.

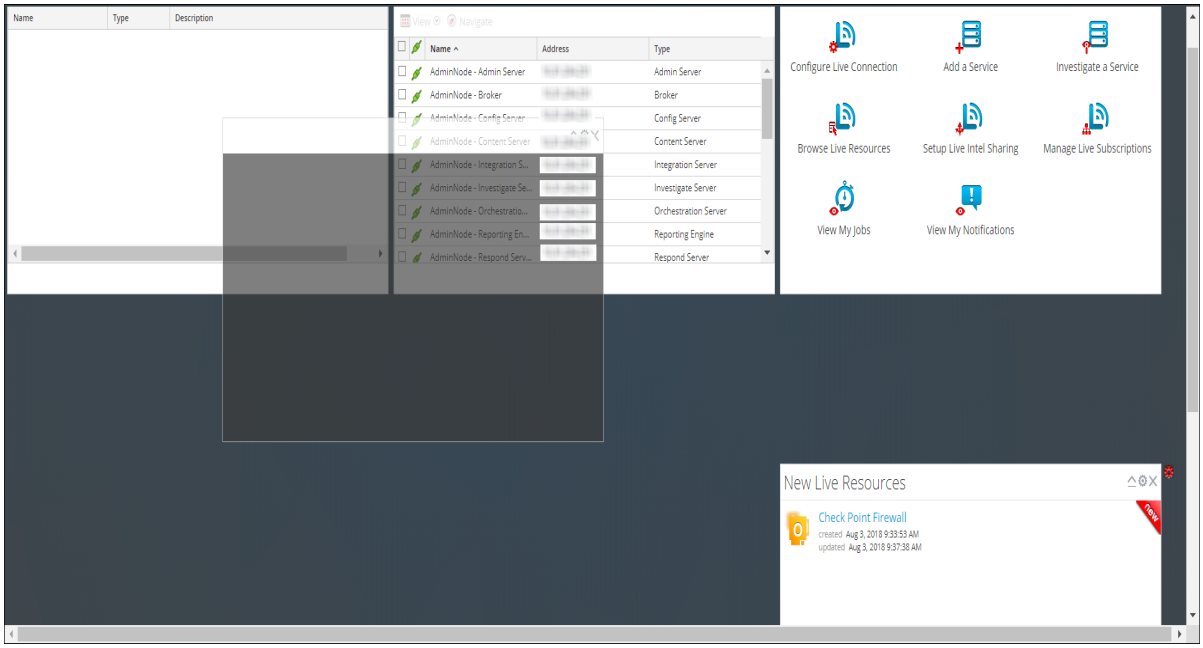
For more information on available dashlets, see the Dashboards Catalog in the NetWitness Content space on NetWitness Community.

Rearrange a Dashlet

You can arrange dashlets according to your preference by dragging and dropping them into a different order on the dashboard.

1. To move a dashlet, hover in the header of the dashlet that you want to move.
   The directional cursor appears over the dashlet. Click and hold in the header of the dashlet that you want to move.

2. Continue to hold the left mouse button and drag the window toward the new location.
   The figure below shows a dashlet as it is being re-arranged.



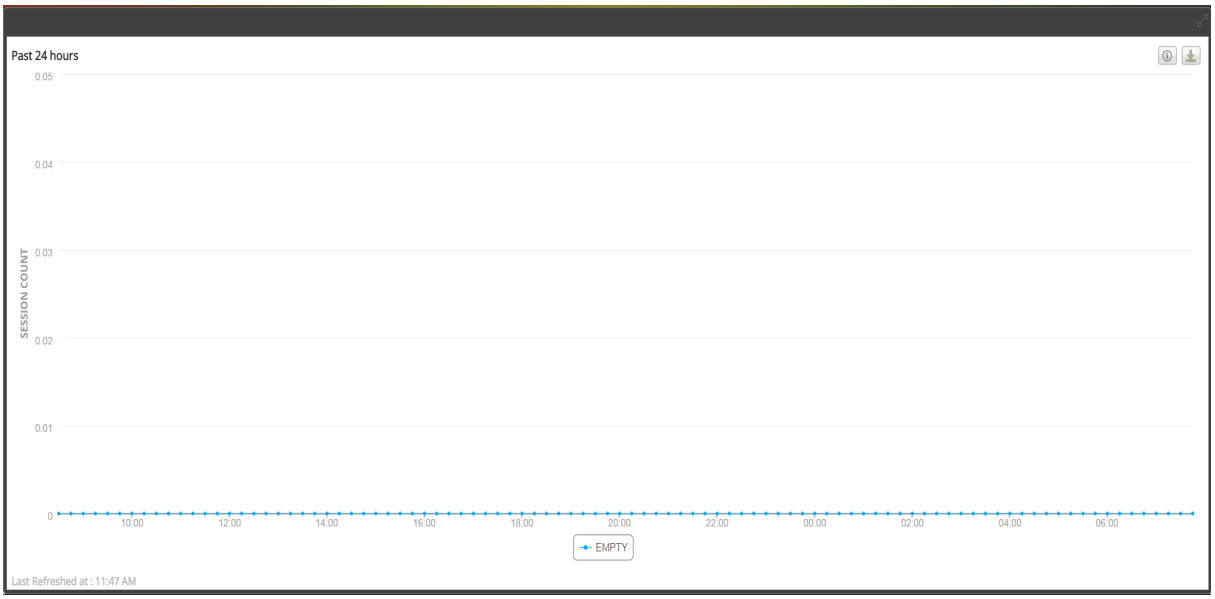
3. Release the mouse button when the dashlet is in the desired location.
   The dashlet that currently occupies that position moves down.

Maximize a Single Dashlet

This section explains how to open a dashlet on the entire area of the main NetWitness dashboard with the same dashlet title. Dashlets that have a lot of columns or charts, for example some Reporting dashlets, are easier to view when maximized so that the entire contents is visible without scrolling.

To maximize a dashlet, click the maximize control icon in the dashlet title bar: ⤢. The dashlet is displayed on full screen.

To minimize a dashlet, click the same control icon in the dashlet title bar: ⤢. The dashlet is restored to previous size.



Delete a Dashlet

1. Click ✕ in the dashlet title bar:
   A confirmation pop-up is displayed to confirm if you want to delete the dashlet.
2. Click **Yes**, if you want to delete. The dashlet is removed from the dashboard.
   Click **No**, if you do not want to delete.

Note: After you remove the dashlet, the empty space is replaced by a placeholder where you can add another dashlet using the above Add a Dashlet procedure.

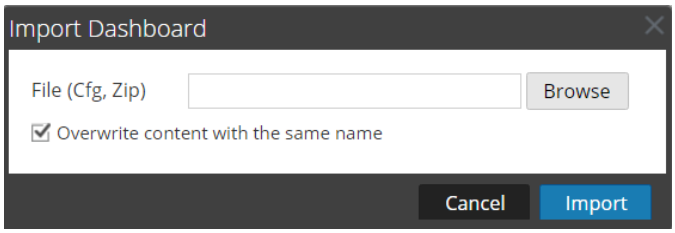
Importing and Exporting Dashboards

The ability to customize dashboards to changing circumstances and conditions could result in a large number of dashboards that are not needed on a daily basis. Rather than reinvent the wheel each time you want to recreate a particular custom dashboard, you can export your dashboards that are not currently in use. When you are ready to use a previously exported dashboard, import the dashboard into NetWitness.

Import a Dashboard

Note: You can import the Reporter Realtime Charts dashboard and its related charts in different instances of the NetWitness server and Reporting Engine from which it was exported.

1. In the dashboard toolbar, click (Import Dashboard).
   The Import Dashboard dialog is displayed.



2. Browse to the dashboard file in the **Import Dashboard** dialog. You can import .cfg and .zip files.
3. Click **Import**.
   The dashboard is displayed in NetWitness

Export a Dashboard

Note: When you export a Reporter Realtime dashboard, the corresponding Reporting Engine contents is also exported.

Exported dashboards are designed to work within the same NetWitness instance. It is also possible to share your custom dashboards with other users in your organization, provided they have equivalent permissions.

To export a dashboard, you must have the dashboard open to access the Export Dashboard option under the Edit drop-down menu in the dashboard toolbar.

1. Navigate to the dashboard that you want to export. All existing dashboards appear in the drop-down **Dashboard Selection List** in the currently displayed dashboard.
2. In the dashboard toolbar, click  (Export Dashboard).
   The exported file is saved in .zip format.

Note: The Export feature is not applicable for preconfigured dashboards.

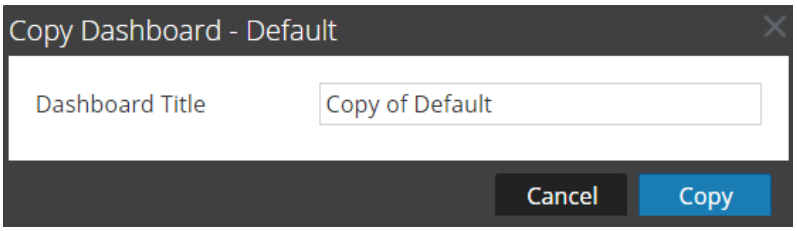
Copying a Dashboard

To customize the views in NetWitness, you can copy dashboards to the NetWitness dashboard or a custom dashboard. The NetWitness dashboard, as the name suggests, offers all NetWitness dashlets. The Copy Dashboard dialog creates a duplicate dashboard, which can be customized. When you copy a dashboard, the default name is prefixed with `Copy of`. For example, if the name of the original dashboard is `XYZ`, the default title of the copied dashboard will be `Copy of XYZ`.

To copy a dashboard:

1. Navigate to any dashboard.
2. In the dashboard toolbar, click  .
   The Copy Dashboard dialog is displayed. The following screenshot is an example of copying a

dashboard.



3. Enter the Dashboard Title.
4. Click **Copy**.

Sharing a Dashboard

In NetWitness, as an administrator you can share dashboards for viewing purposes with other roles such as Administrators, Analysts, Operators and so on. When you share a dashlet, the users can only view the dashboard, make dashboard as favorite, copy the dashboard, and export the dashboard. In case of other roles such as Analysts, Operators, and so on, you can share the dashboard only with similar roles. For example, an analyst can share a dashboard with other analysts only.

1. Navigate to any dashboard.
2. In the dashboard toolbar, click 

and select the checkbox of the role with whom you want to share the dashboard.

Note: If you do not want to share the dashboard, clear the checkbox of the role. If a dashboard is shared, the dashboard name will be displayed with the share icon .

Removing Unwanted Dashboards

You can remove the following dashboards by enabling the dashboard cleaning job.

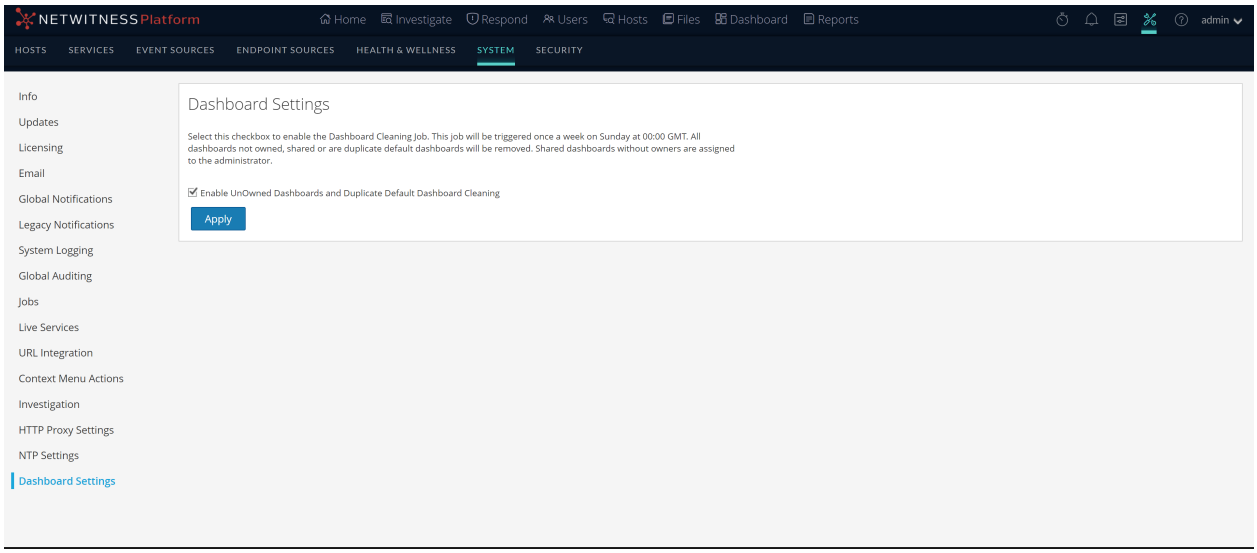
- Dashboards not owned by anyone
- Dashboards not shared
- Duplicates default dashboards

When the dashboard cleaning job is enabled, a scheduled job is triggered once a week on Sunday at 00:00.

Shared dashboards without owners are assigned to the administrator.

To enable Dashboard Cleaning Job:

1. Go to **(Admin) > System > Dashboard Settings**.
2. Select the **Enable UnOwned Dashboards and Duplicate Default Dashboard Cleaning** checkbox.
3. Click **Apply**.



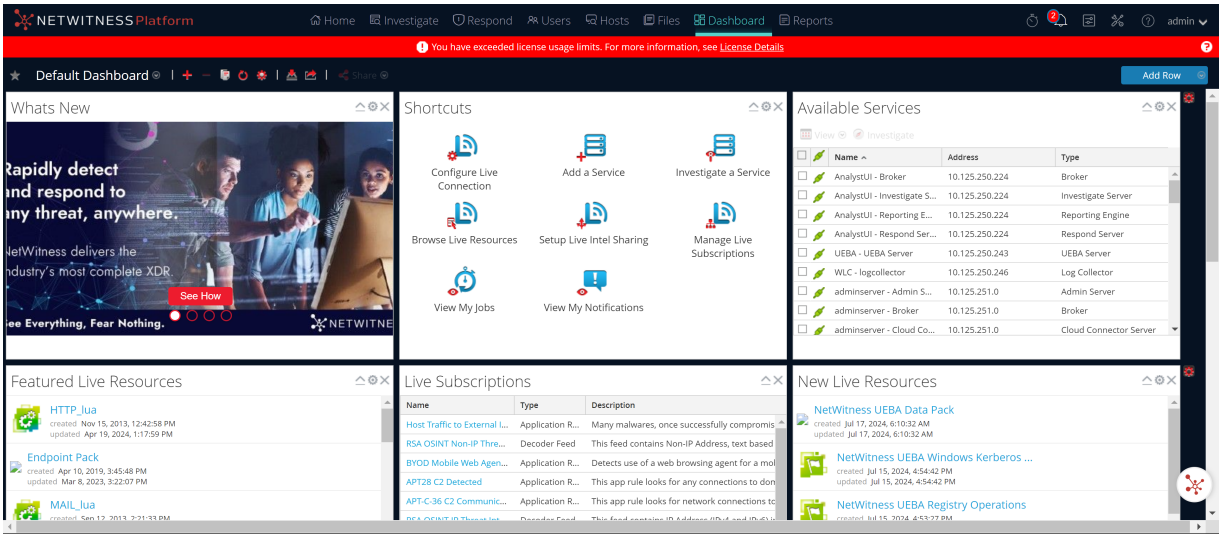
Using Dashboards in the Analyst User Interface

Large environments that include geographical distribution with a single data center and multiple NetWitness Servers require Analyst UI instances in all their NetWitness locations or managed entities. For example, if an Analyst UI is deployed for the EMEA SOC team, analysts can query their EMEA NetWitness Platform hosts directly. If the EMEA team has Broker hosts and Concentrator hosts within the region, the Analyst UI can connect and query them instead of connecting back to Primary User Interface (Primary UI).

When using the dashboards in the Analyst UI, these features apply and affect the dashboards available to analysts:

- Each Analyst UI instance is connected to its local Reporting Engine service. Every Reporting Engine has its own copy of the built-in content such as rules and charts and the local Reporting Engine runs them on the default data source (if configured in Reporting Engine) when the dashboard is enabled.
- The built-in Reporting Engine content that is modified on local Analyst UI is available only to that specific Analyst UI. This behavior is same for an Admin UI as well.
- Dashboards that are shared across different Analyst deployments display the Reporting Engine chart data from the shared instance. To edit the shared dashboard, the analyst must create a copy or contact the Admin to customize it.
- When built-in preconfigured dashboards are enabled from an Admin UI, the dashboard is enabled for all the roles and for all the Analyst UIs. However, the data displayed in every Analyst UI is specific to the associated Reporting Engine.
- By default, all the built-in preconfigured dashlets are disabled and can be enabled only from an Admin UI. Before you enable a preconfigured dashlet, you must set up the Live Services Account, see

the *Set Up Live Services* topic in the Live Services Management Guide.



Note: The Analyst UI functions are similar to the Admin UI functions, except all configurations must be performed from the Admin UI.

Setting User Preferences

You can view and manage your NetWitness global application preferences from your user profile. There are two global user preference dialogs that have different options. The user Preferences dialog is accessible from the Home, Springboard, Investigate (Events), Respond, Users, Hosts, Files and Configure views. The Preferences dialog is accessible from the Investigate, Dashboard, Reports,  (Configure) , and  (Admin) views. The dialog that you see depends on where you access the user preferences.

You can:

- Change the application language
- Set the application time zone
- Set the application date and time format*
- Select your default NetWitness starting location*
- Select your default Investigate view*
- Choose a dark or light theme for the application*
- Change your password (See Changing Your Password for more information.)
- Enable or disable notifications**
- Enable or disable context menus**

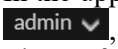
* You can make this change from the **User Preferences** dialog accessible from these views: Home, Springboard, Investigate > Events (formerly Event Analysis), Respond, Users, Hosts, Files, and  (Configure) > (Capture Policies, Incident Rules, Incident Notifications, and Log Parser Rules). See User Preferences.

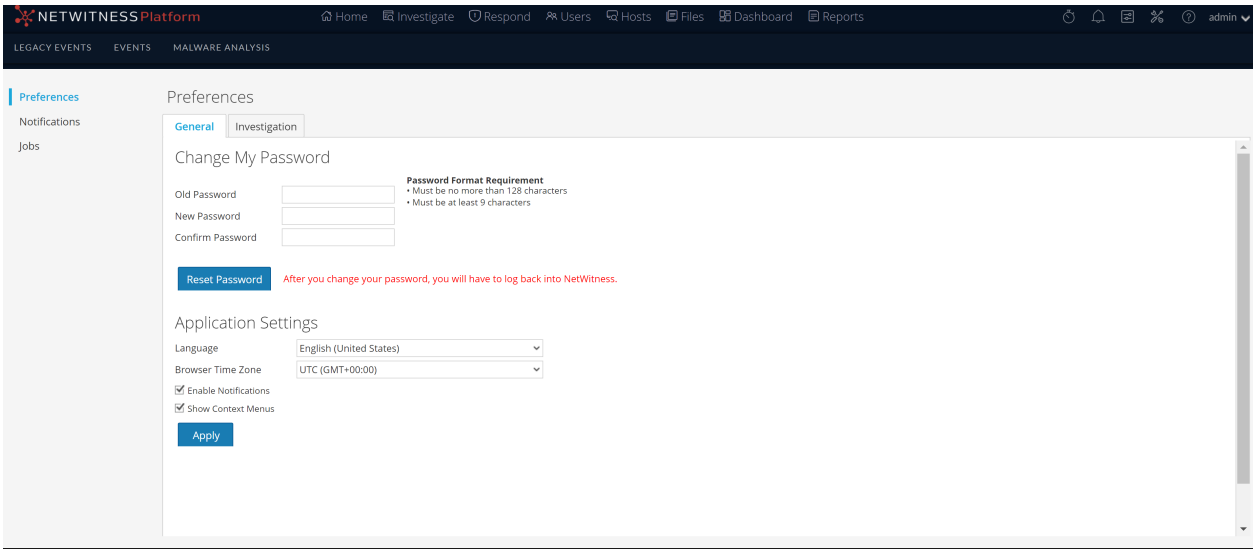
** You can make this change from the **Preferences** dialog accessible from these views: Investigate, Dashboard, Reports,  (Configure) > (Live Content, Subscriptions, ESA Rules, and Custom Feeds), and  (Admin) . See Preferences.

Preferences

This section gives instructions for various tasks that can be performed in the Preferences dialog that is accessible in Investigate, Dashboard, Reports,  (Configure) , and  (Admin) .

View your Preferences

In the upper right corner of the NetWitness browser window, select your username, for example  , and then select **Profile**.
The Preferences dialog shows your current preferences.



Set the Language and Time Zone

You can change your preferred language for the entire NetWitness Platform. The default language is English (United States).

1. In the Preferences dialog, select your localization preferences:
   a. **Language**: Select your preferred language for NetWitness.
   b. **Browser Time Zone**: Set the time zone to use in the NetWitness.
2. Click **Apply**.
   Your preferences become effective immediately.

Note: When Daylight Saving Time (DST) starts or ends, if the selected time zone for the currently logged in user observes DST, the user interface automatically updates to reflect the correct time.

Enable or Disable System Notifications for Your User Account

By default, NetWitness system notifications are enabled when a new user account is created. You can disable and enable these notifications at any time.

1. In the Preferences dialog Application Settings section:
   - To enable notifications for your user account, select the **Enable Notifications** checkbox.
   - To disable notifications, clear the **Enable Notifications** checkbox.
2. Click **Apply**.
   Your preference becomes effective immediately.

Enable or Disable Context Menus for Your User Account

By default, context menus are enabled when a new user account is created. Context menus provide additional functions for specific views when you right-click a view.

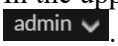
1. In the Preferences dialog Application Settings section:
   - To enable context menus for your user account, select the **Show Context Menus** checkbox.
   - To disable context menus, clear the **Show Context Menus** checkbox.
2. Click **Apply**.
   Your preference becomes effective immediately.

Note: Settings available on the Investigate tab in the Preferences dialog are documented in the *NetWitness Investigate User Guide*.

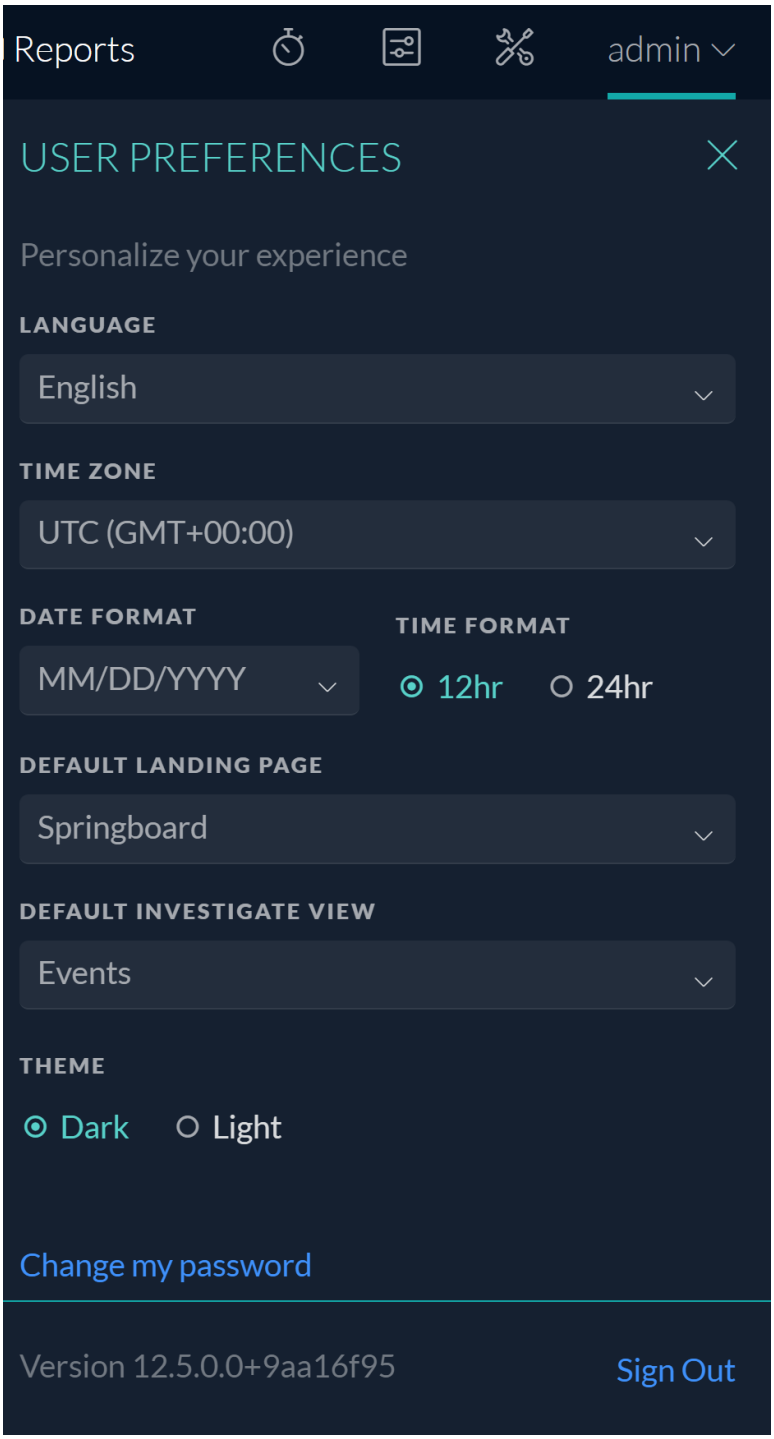
User Preferences

This section gives instructions for various tasks that can be performed in the User Preferences dialog that is accessible in the Springboard, Events, Respond, Users, Hosts, Files and  (Configure) views.

View Your User Preferences

In the upper right corner of the NetWitness browser window, select your username, for example, 

.
The User Preferences dialog shows your current preferences when accessed through the Home, Springboard, Events, Respond, Users, Hosts, Files and  (Configure) views.



Any selections that you make become effective immediately.

Set the Language, Time Zone, and Date and Time Format

You can change your preferred language for the entire NetWitness Platform UI. The default language is English (United States). You can also change the time zone and the format of the date and time for your location.

1. Open the User Preferences dialog.
2. In the User Preferences dialog, select your localization preferences:
   a. **Language**: Select your preferred language for NetWitness.
   b. **Time Zone**: Set the time zone to use in the NetWitness.
   c. **Date Format**: Set the format for the order of the display of the month (MM), day (DD), and year (YYYY). For example, the MM/DD/YYYY format shows the date as 05/11/2019.
   d. **Time Format**: Set the time as 12-hour or 24-hour time. For example, 2:00 PM in 12-hour time is 14:00 in 24-hour time.

   Changes in the Investigate and Respond views become effective immediately.

Note: When Daylight Saving Time (DST) starts or ends, if the selected time zone for the currently logged in user observes DST, the user interface automatically updates to reflect the correct time.

Select the Default NetWitness Platform Starting Location

1. Open the User Preferences dialog.
2. In the **Default Landing Page** field, select the opening view that you would like to see when you log in to NetWitness. You can choose Home Page, Springboard, Investigate, Respond, Users, Hosts, Files, Dashboard, Reports, Configure, and Admin, and according to your user role. For example, you can choose Respond to go directly to the relevant section of the application for Incident Responders. For more information, see Setting Up Your Default View by SOC Role to help you select the appropriate default view.
   This selection sets the default view for the entire application. The changes take effect immediately.

Select the Default Investigate View

1. Open the User Preferences dialog.
2. In the **Default Investigate View** field, select the default landing page when you log in to NetWitness and navigate to Investigate. You can choose Navigate, Legacy Events (if enabled), Events (formerly Event Analysis), or Malware Analysis as the default Investigate view. For example, you can choose Events for the default Investigate view to go directly to the Events view to see the events generated for a service. See Setting Up Your Default View by SOC Role to help you select the appropriate default view. For more information, see the *NetWitness Investigate User Guide*.

Note: After you have applied the change in the drop-down, sometimes it takes few seconds for the changes to take effect.

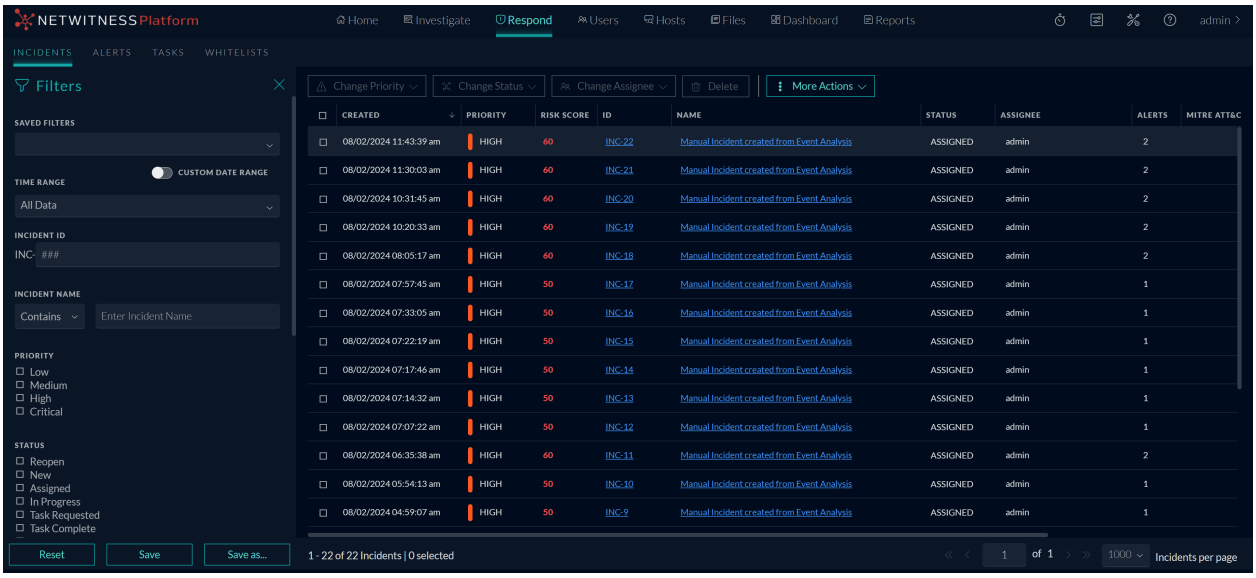
Choose the Appearance of NetWitness Platform

You can choose a dark theme or a light theme for your application, depending on your personal preference. When you change the theme, the Respond view and some Investigate views change to the light or dark theme. Your selection only changes how NetWitness appears to you, not other users.

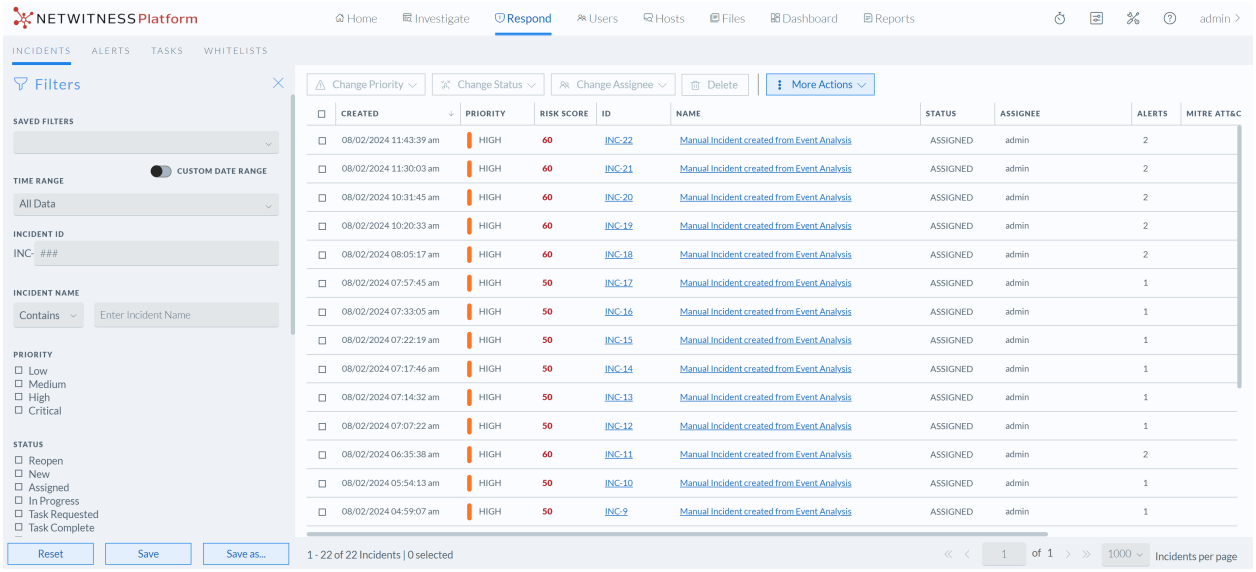
1. Open the User Preferences dialog.
2. Under **Theme**, select one of the following options:
   - **Dark**: The dark theme is best for darker environments or when you do not need as much contrast.
   - **Light**: The light theme is best for lighter environments, when you need more contrast, or when you are projecting the application for others to view. Since some views are not affected by the theme changes, you may want to choose the light theme for a more cohesive viewing experience.

Changes become effective immediately.

The following figure shows the dark theme.



The following figure shows the light theme.


NETWITNESS Platform
Home
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
admin
INCIDENTS
ALERTS
TASKS
WHITELISTS
Filters
SAVED FILTERS
CUSTOM DATE RANGE
TIME RANGE
All Data
INCIDENT ID
INC- ###
INCIDENT NAME
Contains
Enter Incident Name
PRIORITY
Low
Medium
High
Critical
STATUS
Reopen
New
Assigned
In Progress
Task Requested
Task Complete
Reset
Save
Save as...
Change Priority
Change Status
Change Assignee
Delete
More Actions
CREATED
PRIORITY
RISK SCORE
ID
NAME
STATUS
ASSIGNEE
ALERTS
MITRE ATT&C
08/02/2024 11:43:39 am HIGH 60 INC-22 Manual Incident created from Event Analysis ASSIGNED admin 2
08/02/2024 11:30:03 am HIGH 60 INC-21 Manual Incident created from Event Analysis ASSIGNED admin 2
08/02/2024 10:31:45 am HIGH 60 INC-20 Manual Incident created from Event Analysis ASSIGNED admin 2
08/02/2024 10:20:33 am HIGH 60 INC-19 Manual Incident created from Event Analysis ASSIGNED admin 2
08/02/2024 08:05:17 am HIGH 60 INC-18 Manual Incident created from Event Analysis ASSIGNED admin 2
08/02/2024 07:57:45 am HIGH 50 INC-17 Manual Incident created from Event Analysis ASSIGNED admin 1
08/02/2024 07:33:05 am HIGH 50 INC-16 Manual Incident created from Event Analysis ASSIGNED admin 1
08/02/2024 07:22:19 am HIGH 50 INC-15 Manual Incident created from Event Analysis ASSIGNED admin 1
08/02/2024 07:17:46 am HIGH 50 INC-14 Manual Incident created from Event Analysis ASSIGNED admin 1
08/02/2024 07:14:32 am HIGH 50 INC-13 Manual Incident created from Event Analysis ASSIGNED admin 1
08/02/2024 07:07:22 am HIGH 50 INC-12 Manual Incident created from Event Analysis ASSIGNED admin 1
08/02/2024 06:35:38 am HIGH 60 INC-11 Manual Incident created from Event Analysis ASSIGNED admin 2
08/02/2024 05:54:13 am HIGH 50 INC-10 Manual Incident created from Event Analysis ASSIGNED admin 1
08/02/2024 04:59:07 am HIGH 50 INC-9 Manual Incident created from Event Analysis ASSIGNED admin 1
1 - 22 of 22 Incidents | 0 selected
1 of 1
1000
Incidents per page

Managing Jobs

Inevitably, there are on-demand or scheduled tasks in NetWitness that take a few minutes to be completed. The NetWitness jobs system lets you begin a long-running task and continue using other parts of NetWitness while the job is running. Not only can you monitor the progress of the task, but you can also receive notifications when the task has completed and whether the result was a success or failure.

While you are working in NetWitness, you can open a quick view of your jobs from the toolbar. You can look anytime, but when a job status has changed, the Jobs icon ( ) is flagged with the number of running jobs. Once all jobs are completed, that number disappears.

You can also see the jobs in these two views:

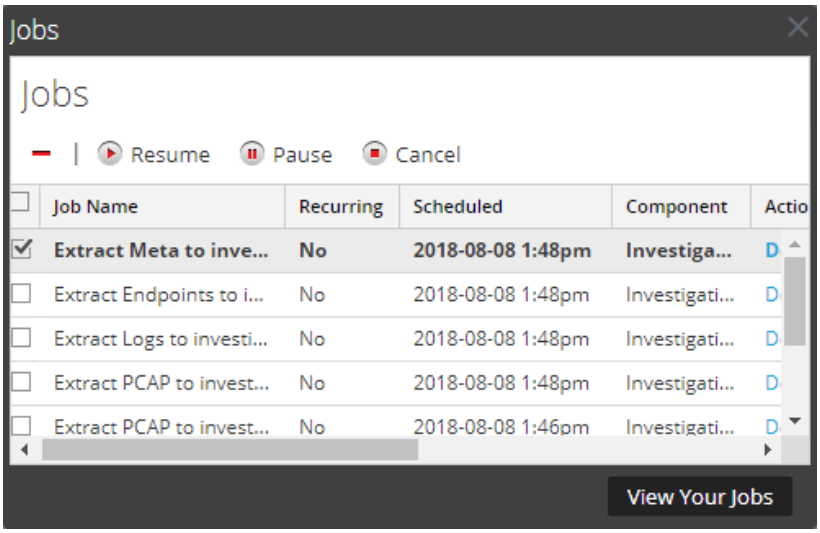
- In the user Profile Jobs panel, you see the same jobs in a full panel. These are only your jobs.
- In the System view, users with administrative privileges can view and manage all jobs for all users in a single jobs panel.

The structure of the jobs panel is the same in all views.

Display the Jobs Tray

In the NetWitness toolbar, click the Jobs icon ( ).

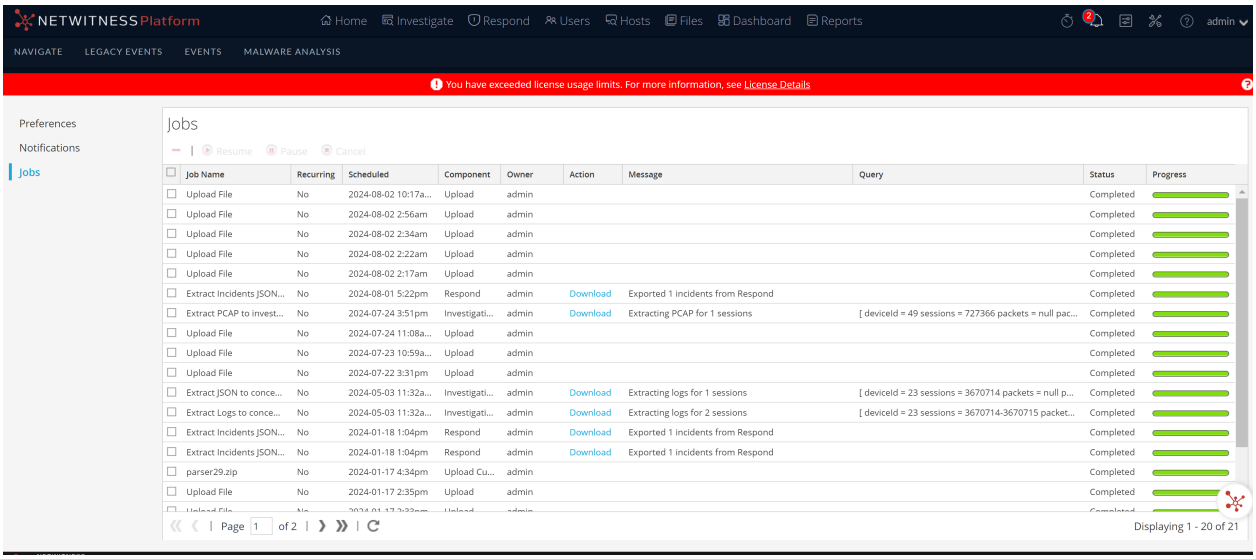
The Jobs Tray is displayed.



The Jobs Tray lists all recurring and non-recurring jobs that you own, using a subset of the columns available in the Jobs panel. Otherwise the Jobs Tray and the user Profile view Jobs panel are the same. In the Admin System view, the Jobs panel lists information about all NetWitness jobs for all users.

View All of Your Jobs

To see a complete view of your jobs, in the Jobs Tray, click **View Your Jobs**.
The Jobs panel is displayed.



Pause and Resume Scheduled Execution of a Recurring Job

The Pause and Resume options apply only to recurring jobs. You can pause a recurring job that is running; however, it has no effect on that execution. The next execution (assuming the job is still paused) is skipped.

1. To stop the next execution of a recurring job, in any **Jobs panel**, select the job, and click **Pause**.
   The next execution of the job is skipped, and the schedule is paused until you click Resume.
2. To restart execution of paused recurring jobs, select the job and click **Resume**.
   The next execution of the job occurs as scheduled, and the schedule for the job resumes.

Cancel a Job

To cancel jobs that are executing or in the queue to execute:

1. In the **Jobs Tray** or either **Jobs** panel, select one or more jobs.
2. Click **Cancel**.
   A confirmation dialog is displayed.
3. Click **Yes**.
   The jobs are canceled, and the entries remain in the list with a status of **canceled**.

   If you cancel a recurring job, it cancels that execution of the job. The next time the job is scheduled to run, it executes normally.

Delete a Job

Caution: When you delete a job, the job is instantly deleted from the list. No confirmation dialog is offered. If you delete a recurring job, all future executions are removed as well.

Users can delete their own jobs before, during, or after execution. Administrators can delete any job. To delete jobs:

1. Select one or more jobs.
2. Click −.
   The jobs are deleted from the list.

Download a Job

When a job has the Download status in the Action column, you can download the result of the job. If you are working in the Investigate view and extract the packet data for a session as a PCAP file or extract the payload files (for example, Word documents and images) from a session, a file is created. To download the file to your local system, click **Download**.

Viewing and Deleting Notifications

While you are working in NetWitness, you can view recent system notifications without leaving the area where you are working. You can open a quick view of notifications from the NetWitness toolbar. You can look anytime, but when a new notification is received, the Notifications icon is flagged ().
Examples of notifications include:

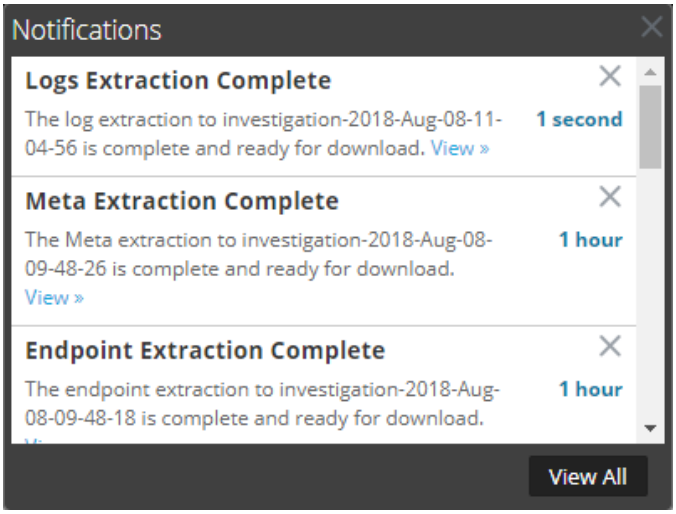
- A host upgrade completed.
- A parser push to decoders completed.
- A newer software version is available.

You can see notifications in these two views:

- In the Notifications tray, you can see your recent notifications.
- In the user Profile Notifications panel, you can view all of your notifications.

View Recent Notifications

To display recent notifications, click the Notifications icon ().
The Notifications tray is displayed.

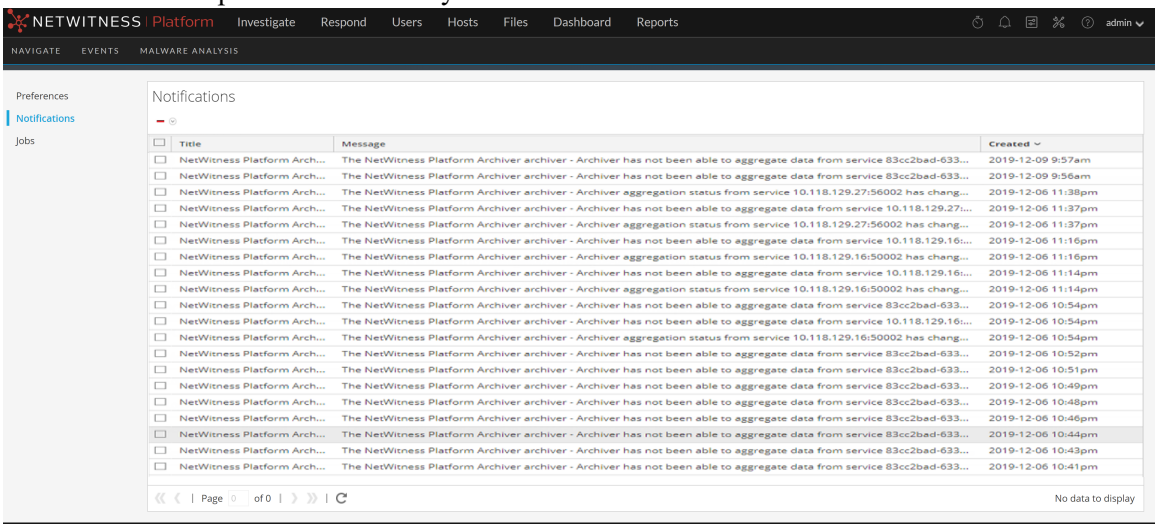


View All Your Notifications

To view all of your notifications, do one of the following:

- Click  to open the Notifications tray and then click **View All** in the Notifications tray.
- In the upper right corner of the NetWitness browser window, select your username and then select **Profile**. In the options panel of the Preferences dialog, select **Notifications**.

The Notifications panel shows all of your notifications.



Delete Notification Records

To delete notification records:

1. In the **Profile Notifications** list, select the notifications that you want to delete.
2. Click −.

   The selected notifications are deleted from this list and from the Notifications tray.

Viewing Help in the Application

There are different ways available to get help while using NetWitness. You can use inline help, tooltips, and online help links.

View Inline Help

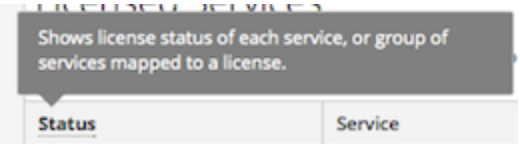
Inline help provides additional information about what to do in sections or fields that you are currently viewing in the NetWitness user interface. To display inline help, hover over . The inline help shows a brief description of the element.

Inline help example:

View Tooltips

Tooltips are a quick way for you to see a description of the text or additional information about an action, field, or parameter. Tooltips appear as underlined text. To display the tooltip and see a brief description of the term, hover over the underlined text.

Tooltip example:

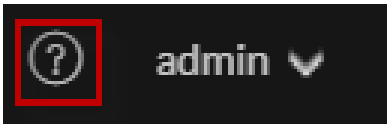


View Online Help

Online help links take you outside of NetWitness to the NetWitness Community online documentation. This site has a complete documentation set for NetWitness, and the links take you directly to the topic that describes the part of the user interface currently in view.

To view the online help topic for the current location, click in the NetWitness toobar or in a dialog. The relevant help topic is displayed in a separate browser window. The topic describes the features and functions of the current view or dialog. From that topic, you can quickly navigate to the related procedures.

The following figure is an example of the online help icon in the NetWitness toobar.



Finding Documents on NetWitness Community

The NetWitness documentation is located on NetWitness Community. NetWitness Community brings all of your NetWitness resources together in one place. It includes advisories, product documentation, knowledge base articles, downloads, and training. To view a *Guided Tour of NetWitness Community*, see https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness.

Locate NetWitness Documentation

NetWitness Logs, Networks, Endpoints, and UEBA documentation is at the following link: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation

To navigate to NetWitness Logs, Networks, Endpoints, and UEBA documentation:

1. On the NetWitness Community homepage (https://community.netwitness.com), under **Products**, click **NetWitness Platform**.
2. On the NetWitness Platform page, click **Documentation**.

Locate NetWitness Content

NetWitness Content contains feeds, parsers, reports, and rules. It is located at the following link: https://community.netwitness.com/t5/threat-intelligence/ct-p/threat-intelligence.

To navigate to NetWitness Content:

1. On the NetWitness Community homepage (https://community.netwitness.com), under **Products**, click **NetWitness Platform**.
2. On the NetWitness Platform page, click **Documentation** > **Threat Intelligence**.

Locate NetWitness Supported Event Sources

The NetWitness Integrations Catalog is located at the following link: https://community.netwitness.com/t5/netwitness-platform-integrations/tkb-p/netwitness-integrations.

To navigate to the NetWitness Integrations Catalog:

1. On the NetWitness Community homepage (https://community.netwitness.com), under **Products**, click **NetWitness Platform**.
2. On the NetWitness Platform page, click **Integrations**

Locate Hardware Setup Guides

The Hardware Setup Guides are at the following link: https://community.netwitness.com/t5/netwitness-platform-hardware/tkb-p/netwitness-hardware-documentation.

1. On the NetWitness Community homepage (https://community.netwitness.com), under **Products**, click **NetWitness Platform**.
2. On the NetWitness Platform page, click **Documentation** > **Hardware Setup Guides**.

Follow Content for Updates

You can follow pages or documents to be notified of changes.

1. Log in to NetWitness Community.
2. Navigate to a page or a document and next to the Search bar, click ⋮ > **Subscribe**.

NetWitness Educational Services

Sign up for access to NetWitness courses and additional resources on the NetWitness Educational Services and Training.

NetWitness Education Portal	https://netwitness.sabacloud.com/Saba/Web_spf/NA10P2PRD088/guestapp/home;spf-url=guest%2Fguestlearningcatalog
NetWitness Educational Services Course Catalog	https://community.netwitness.com/t5/netwitness-education-courses/tkb-p/netwitness-training
NetWitness Educational Services Training Schedule	https://community.netwitness.com/t5/netwitness-education-blog/netwitness-instructor-led-training-schedule/ba-p/655826
NetWitness Educational Services Support Contact	education.support@netwitness.com

Send Your Feedback to NetWitness

Your feedback is very important to us and helps us to provide a better experience for our customers. Please send your suggestions to feedbacknwdocs@netwitness.com

Troubleshooting the User Interface

This section describes common issues that users may face during setup and provides basic troubleshooting information.

Basic Troubleshooting Tips for User Setup

The following table provides basic troubleshooting tips that may be helpful for user setup in NetWitness.

Problem	Troubleshooting Tip
When I log in to NetWitness, I see the wrong default view.	Verify that the correct default view is set in the Default Landing Page field in your user preferences. If you select the Dashboard view, you can select the predefined dashboard that is most appropriate for your SOC role. You can also import or create your own dashboard.
I see the correct view, but the metadata does not load.	Make sure that you are using the latest version of the browser. If that does not work, try using another browser. For example, if you are using Safari, try using Firefox or Chrome.
I am using Internet Explorer 10 and I get the following error: `The page can't be displayed.`	NetWitness supports current versions of Firefox, Chrome, and Safari. Internet Explorer is no longer supported.
When I log in, I cannot see anything.	See your administrator, you may need a user role assigned to your account or additional troubleshooting.
I can't see where to change my default landing page.	Go to the User Preferences in the Respond view or Events view (formerly Event Analysis view) or see your administrator.

Analyst User Interface Dashlet Issue

Problem	Cause	Solution
I see the following error message on my dashboard: `The underlying chart for this dashlet is unavailable.`	This scenario occurs on an Analyst UI deployment when an Analyst creates a dashboard on one NetWitness Server, logs in to another NetWitness Server, and tries to view a dashboard that the Analyst did not share.	Share the dashboard to view the data. For more information, see Sharing a Dashboard.

Springboard Issue

Problem	Cause	Solution
I see the following error message on a Springboard panel: `Filter definition is missing! Edit the panel to remove the filter or update with a new filter.`	A query profile that is used to filter events in the panel may have been deleted in the Investigate view. Springboard panels that use a deleted query profile as a filter do not work.	Edit the Springboard panel to remove the filter or use a different filter. For more information, see Managing the Springboard.

Springboard Fails to Load the Panel Issue

Problem	Cause	Solution

I see the following error messages on a Springboard panel: `Request timed out! Contact your administrator or refer to the Getting Started Guide on NetWitness Community for details.`
 	
`Failed to fetch the results. Refresh the panel. If the issue persists, contact your administrator or refer to the Getting Started Guide on NetWitness Community for details.`
	• The Springboard panels request time out in 60 seconds.
	• The associated data sources are offline or not reachable.
	• Allocated memory is insufficient to execute the query.
		• Limit the results by narrowing the time range for the Springboard using the time range field above the panels.
		• Go to the Investigate > Events view and refine the Query Profile used in the panel as described in "Use Query Profile to Encapsulate Common Areas of Investigation" in the *Investigate User Guide*.
		• Make sure that the associated data sources are online.
		• Increase the memory by modifying the `max.query.memory` parameter setting.
		• If the above solution does not work and if the issue still persists, check the service logs in the given order:
		  ▪ Admin server
		  ▪ Investigate server
		  ▪ Respective core services
		
		For more information, see “Display System and Service Logs” section in the *System Maintenance Guide*.

Inconsistent Event Panel Count Issue

Problem	Cause	Solution
Event count on the panel is inconsistent.	The underlying data sources are offline or not reachable.	Make sure that all underlying data sources are online and refresh the panel. For more information, see Managing the Springboard.

NetWitness Platform Getting Started References

The following section contains user interface reference information related to getting started with the NetWitness application.

- User Preferences
- Notifications Panel and Notifications Tray
- Jobs Panel and Jobs Tray

User Preferences

To adjust NetWitness to best fit your environment and work practices, you can set your own global application preferences. You can:

- Change the application language
- Set the application time zone
- Set the date and time formats
- Select your default NetWitness starting location
- Select your default Investigate view
- Choose a dark or light theme for the application
- Change your password
- Enable notifications
- Enable context menus
- Change Investigate preferences - Described in the *NetWitness Investigate User Guide*.

Your global preference options vary depending on whether you access them, such as Springboard, Investigate, Respond, Users, Hosts, Files, Dashboard, Reports, Configure, and Admin. There are two global user preferences dialogs accessible from the main menu bar:

- **User Preferences** dialog - Accessible from these views: Springboard, Investigate > Events (formerly Event Analysis), Respond, Users, Hosts, Files, and  (Configure) > (Capture Policies, Incident Rules, Incident Notifications, and Log Parser Rules).
- **Preferences** dialog - Accessible from these views: Investigate, Dashboard, Reports,  (Configure) > (Live Content, Subscriptions, ESA Rules, and Custom Feeds), and  (Admin) .

What do you want to do?

Role	I want to ...	Show me how
All	Change my Password	Change My Password Section
All	Choose my Default Landing Page	Setting Up Your Default View by SOC Role
All	Set my User Preferences	Setting User Preferences

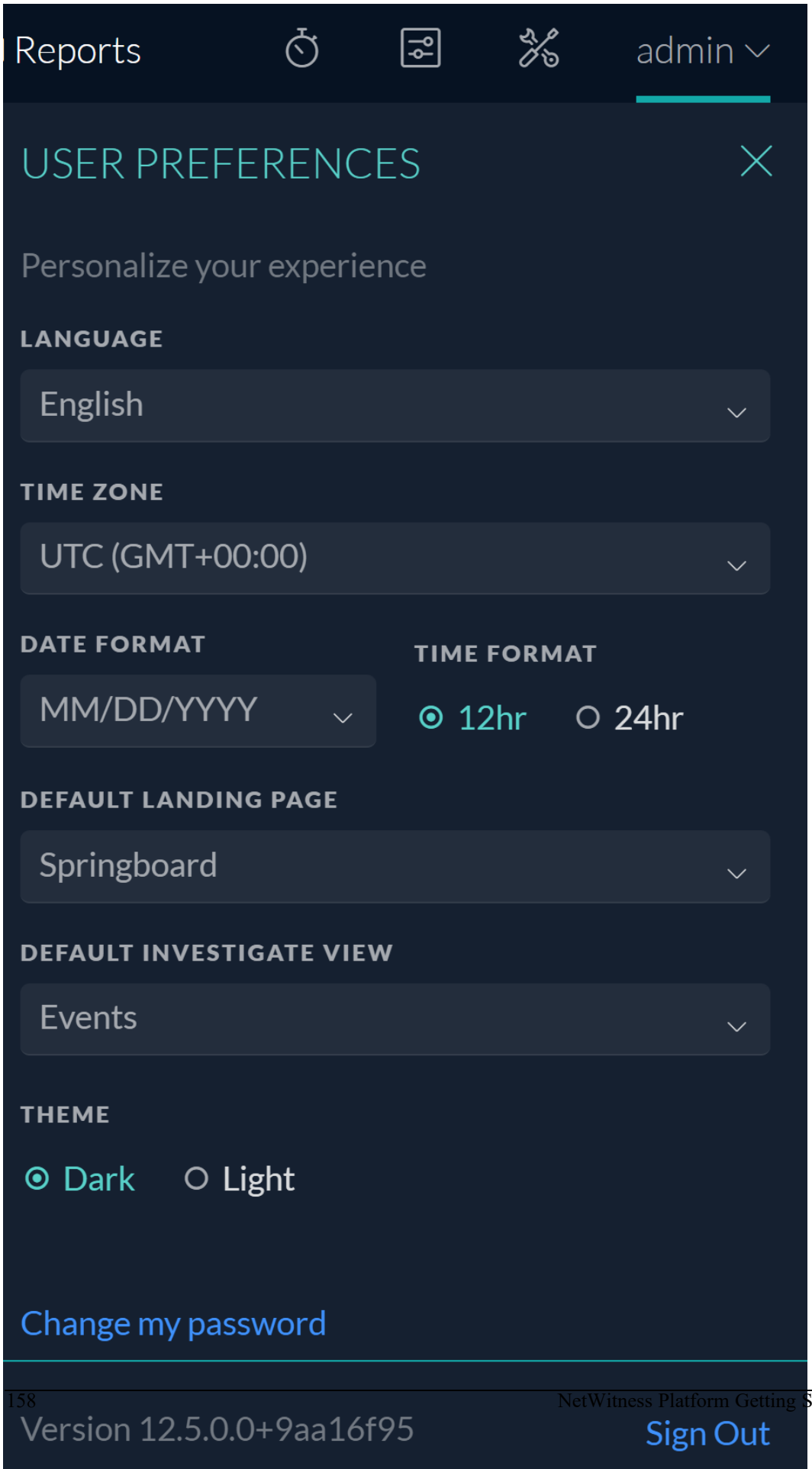
Related Topics

- NetWitness Platform Basic Navigation

User Preferences

To access your user preferences, click your username, for example, 

.
The User Preferences dialog shows your current preferences and the NetWitness version.


Reports
admin
USER PREFERENCES
Personalize your experience
LANGUAGE
English
TIME ZONE
UTC (GMT+00:00)
DATE FORMAT
MM/DD/YYYY
TIME FORMAT
12hr
24hr
DEFAULT LANDING PAGE
Springboard
DEFAULT INVESTIGATE VIEW
Events
THEME
Dark
Light
Change my password
Version 12.5.0.0+9aa16f95
Sign Out

The following table describes the global application preference options that you can access from the User Preferences dialog.

Option	Description
Language	Sets the preferred language for the entire NetWitness Platform. The default language is English (United States).
Time Zone	Sets the time zone to use in NetWitness.
Date Format	Sets the format for the order of the display of the month (MM), day (DD), and year (YYYY). For example, the MM/DD/YYYY format shows the date as 05/11/2017.
Time Format	Sets the time as 12-hour or 24-hour time. For example, 2:00 PM in 12-hour time is 14:00 in 24-hour time.
Default Landing Page	Enables you to select the default view when you log in to NetWitness. You can choose Home Page (From NetWitness 12.5 or later), Springboard, Investigate, Respond, Users, Hosts, Files, Dashboard, Reports,  (Configure) , and  (Admin) , according to your user role. For example, you can choose Respond to go directly to the relevant section of the application for Incident Responders. This selection sets the default view for the entire application.
Default Investigate View	Select the default landing page for the Investigate view. You can choose Navigate, Legacy Events (if enabled), Events, or Malware Analysis as the default Investigate view. For example, you can choose Events for the default Investigate view to go directly to the Events page to view the events generated for a service.
Theme	Changes the appearance of the Respond view and some Investigate views that you see in the application. You can choose between light and dark themes: • **Dark**: The dark theme is best for darker environments or when you do not need as much contrast. • **Light**: The light theme is best for lighter environments, when you need more contrast, or when you are projecting the application for others to view. Since some views are not affected by the theme changes, you may want to choose the light theme for a more cohesive viewing experience. Your selection only changes how NetWitness appears to you, not other users.
Change my password	Opens the Preferences dialog where you can change your password.
Version	Shows the NetWitness version.
Sign Out	Enables you to log out of NetWitness.

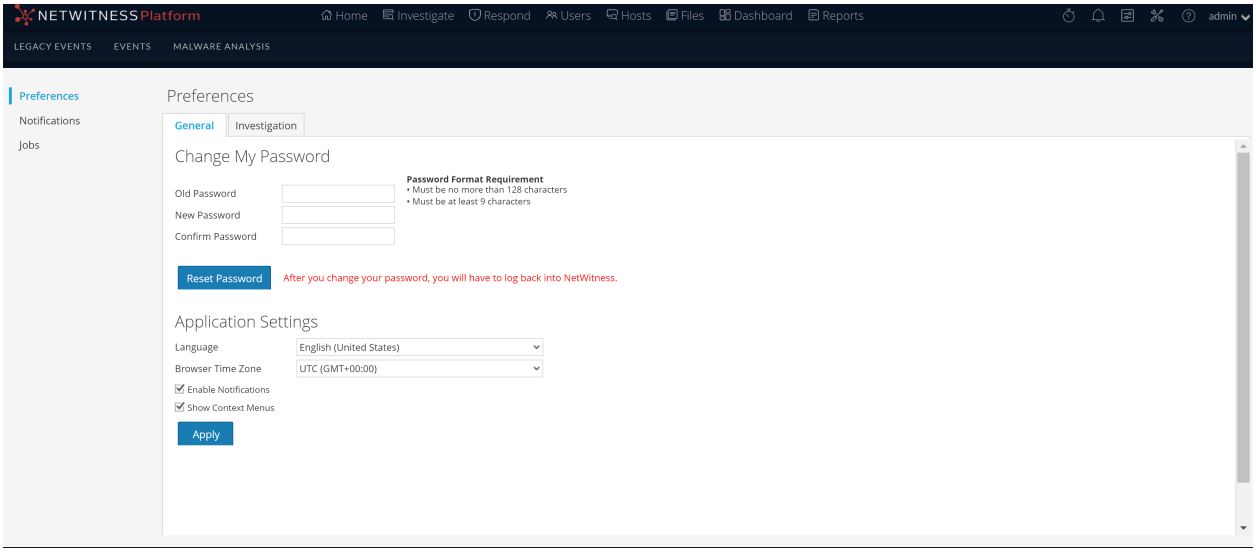
Any selections that you make become effective immediately.

Preferences

To access additional global user preferences, do one of the following:

- For most views, such as Investigate, Dashboard, Reports, (Configure) , or (Admin) , select your username and then select **Profile**.
- In the Home, Springboard, Investigate view [Events (formerly Event Analysis)], Respond, Users, Hosts, Files, and some (Configure) views, select your username, for example admin, and in the User Preferences dialog click **Change my password**.

The Preferences dialog shows your current preferences.



The following tables describe the global application preference options that you can access from the Preferences dialog.

Change My Password Section

This section enables you to change your password. Your administrator defines the appropriate password strength requirements for your NetWitness password, such as minimum password length and minimum number of uppercase, lowercase, decimal, non-Latin alphabetic, and special characters. These requirements are then displayed when changing your password.

The following tables describes the options in the Change My Password section.

Option	Description
Old Password	Enter the password that you used to log in to NetWitness.
New Password	Enter the password that you want to use for the next login.
Confirm Password	Retype the new password.

Option	Description
Reset Password	Updates your user profile with the new password. You will be logged out of NetWitness for the changes to take effect. The new password becomes effective the next time you log in to NetWitness. The password change is applied to your system login and to all NetWitness services on which your account has been added.

If you changed your password, you will be logged out of NetWitness for the changes to take effect. The new password becomes effective the next time you log in to NetWitness.

Application Settings Section

The following tables describes the options in the Application Settings section.

Option	Description
Language	Sets the preferred language for the entire NetWitness Platform. The default language is English (United States).
Browser Time Zone	Sets the time zone to use in NetWitness. Your time zone preference is displayed on the toolbar.
Enable Notifications	This checkbox enables and disables notifications for your user account. By default, NetWitness system notifications are enabled when a new user account is created.
Enable Context Menus	This checkbox enables and disables context menus for your user account. By default, context menus are enabled when a new user account is created. Context menus provide additional functions for specific views when you right-click in a view.
Apply	Updates your preferences and applies the changes immediately.

Notifications Panel and Notifications Tray

NetWitness provides system notifications to advise users about certain actions or conditions:

- A host upgrade completed.
- A parser push to decoders completed.
- A service went down (critical log of a certain type).
- A visualization completed.
- A report completed.
- A newer software version is available.

While you are working in NetWitness, you can view recent system notifications without leaving the area where you are working. You can open a quick view of notifications from the NetWitness toolbar. You can look anytime, but when a new notification is received, the Notifications icon is flagged ().

When you are viewing notifications in the Notifications tray, only recent notifications are displayed. You can access all of your notifications from your user Profile and from the Notifications tray by selecting the View All option. Procedures for viewing notifications are provided in Viewing and Deleting Notifications.

Note: In the Analyst UI, the license notifications are not displayed in the notification tray or login window when the license goes out of compliance or when the license expires. This is displayed only on the Admin UI.

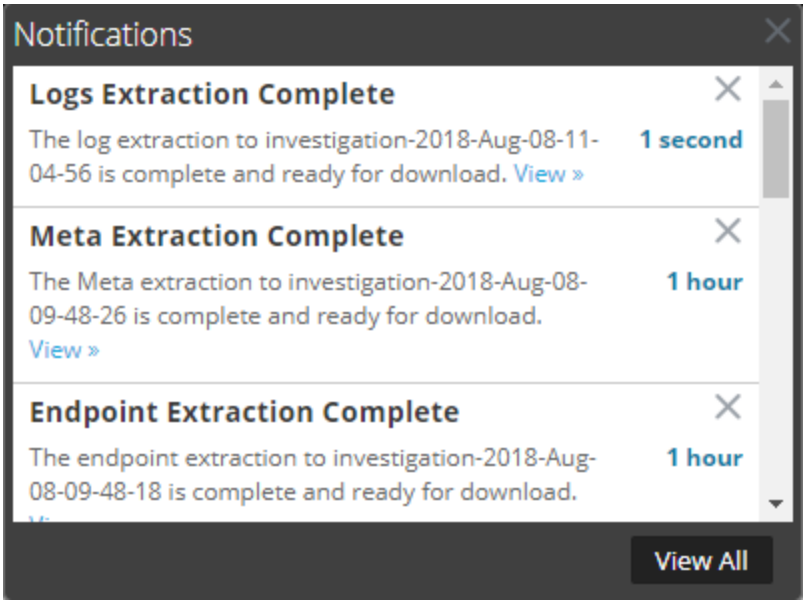
What do you want to do?

Role	I want to ...	Show me how
All	View all notifications	Viewing and Deleting Notifications
All	Delete notifications	Viewing and Deleting Notifications

Quick Look

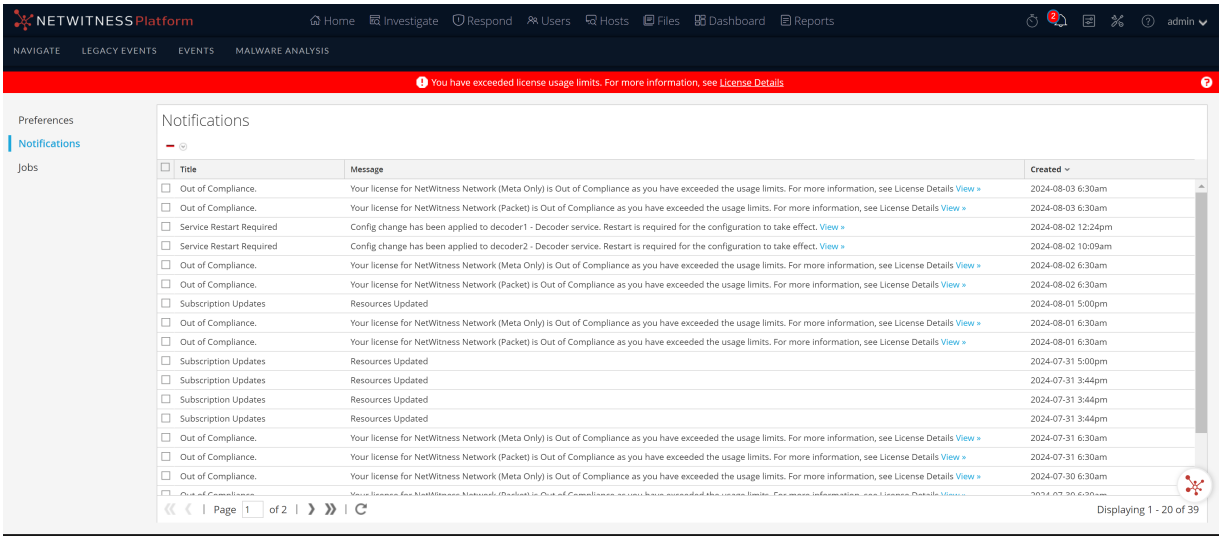
To access the Notifications panel, do one of the following:

- Click  to open the Notifications tray and then click **View All** in the Notifications tray.



- In the upper right corner of the NetWitness browser window, select your username and then select > **Profile**. In the options panel of the Preferences dialog, select **Notifications**.

  The Notifications panel is displayed.



The Notifications tray shows your recent notifications. It contains a subset of the information in the Notifications panel. The Notifications panel shows all of your notifications. The following table describes the Notifications panel and Notifications tray features.

Feature	Description
	(Notifications panel only) Displays a drop-down menu where you can delete the selected notification or all of your notifications in the Notifications panel and in the Notifications tray.
Title	The title of the notification, for example, **Logs Extraction Complete**.
Message	The entire message, for example, **The log extraction to Investigation is complete and ready for download.**
View	Some messages include a **View** link that displays a view where you can take action. For example, if there is a file to download, clicking this link opens the Jobs panel, the view where you can download the file.
Created	The date and time the notification was created. In the Notifications tray, it shows the number of hours or days since the notification was created.
View All	(Notification tray only) Opens the Notifications panel, which lists all of your notifications.

Jobs Panel and Jobs Tray

Jobs are started by various NetWitness components; for example, downloading Content Management System (CMS) resources from Live Services and extracting logs, meta, and PCAP files from NetWitness Investigate.

In the  (Admin) > System view, Administrators can manage all NetWitness jobs in the Jobs panel. Other non-administrative users can view their own jobs in the user Profile Jobs panel.

In addition, while working in NetWitness, you can open a quick view of your jobs from the NetWitness toolbar. When a job status has changed, the Jobs icon () is flagged with the number of running jobs. Once all jobs are completed, that number disappears.

In the Jobs panel, you can:

- View and sort the jobs
- Pause or resume a job
- Cancel a job
- Delete a job
- Download a job

The structure of the jobs panel is the same in all views.

What do you want to do?

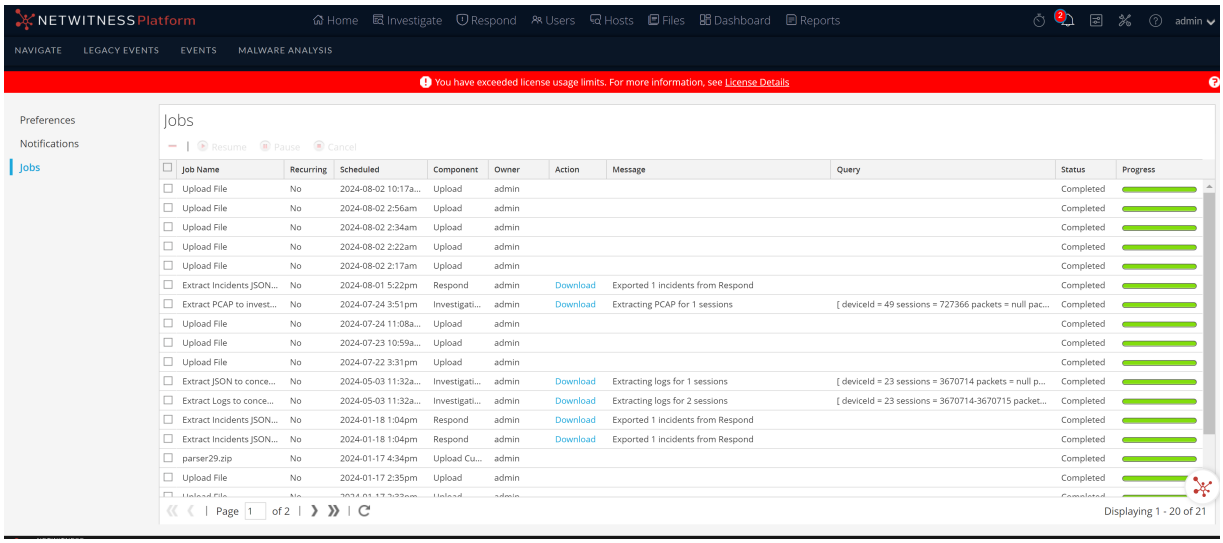
Role	I want to ...	Show me how
All	Pause and Resume a Scheduled Job	Managing Jobs
All	Cancel or Delete a Job	Managing Jobs
All	Download a Job	Managing Jobs

Your actions may be limited to your own jobs depending on your permissions.

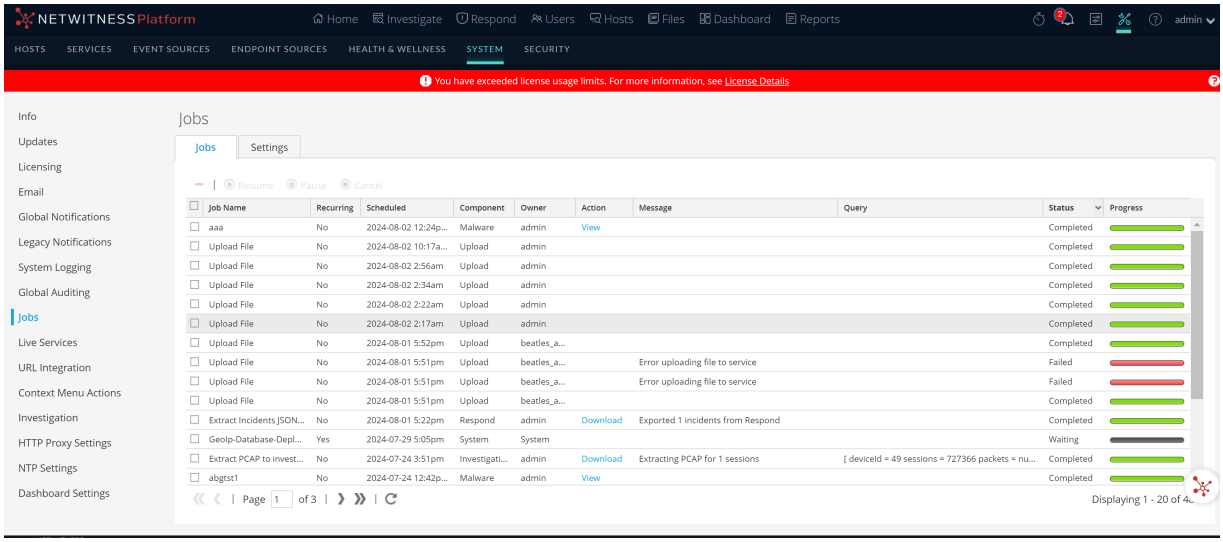
Quick Look

To access the Jobs panel, do one of the following:

- In the upper right corner of the NetWitness browser window, select your username and then select **Profile**. In the options panel of the Preferences dialog, select **Jobs**.
  The Jobs panel is displayed. It shows the jobs of a particular user.

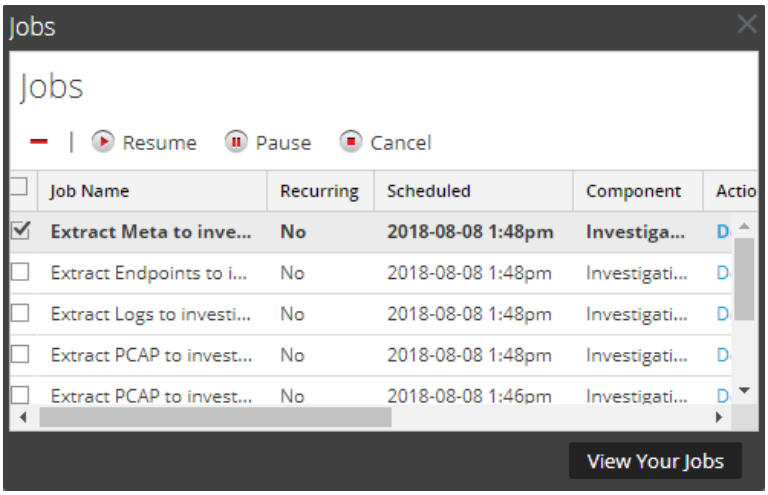


- Go to **(Admin) > System**, and in the options panel, select **Jobs**.
  The Jobs panel in the Admin System view is displayed. It shows the jobs for all users.



The Jobs panel organizes information about jobs into a list. The columns present a job progress bar, the job name, an indication that the job is recurring or not recurring, the NetWitness component that is controlling the job, the owner of the job, the status, any associated message, and a download button to allow downloading of a job's packet capture files or payload files.

To display the Jobs tray, click the **Jobs** icon .



The Jobs tray lists all jobs that you own, recurring and non-recurring, using a subset of the columns available in the **Jobs** panel. Otherwise the Jobs tray and the user Profile Jobs panel are the same. In the Admin System view, the Jobs panel lists information about all NetWitness jobs for all users.

The following table describes the available options in the Jobs panel.

Option	Description
Resume	The Resume option applies only to recurring jobs that have been paused. When you resume a paused job, the next execution of the job executes as scheduled.
Pause	The Pause option applies only to recurring jobs. When you pause a recurring job that is running, it has no effect on that execution. The next execution (assuming the job is still paused) is skipped.
Cancel	Cancels a recurring or non-recurring job. You can cancel a job while it is running. If you cancel a recurring job, it cancels that execution of the job. The next time the job is scheduled to run, it executes normally.
−	Deletes a recurring or non-recurring job from the Jobs panel. When you delete a job, the job is instantly deleted from the Jobs panel. No confirmation dialog is offered. If you delete a recurring job, all future executions are removed as well.

The following table describes the Jobs tray and Jobs panel columns.

Column	Description
Selection box	Enables you to select one or more jobs.
Job Name	Displays the name of the job; for example, **Extract Files** or **Upgrade Service**.
Recurring	Indicates whether the job is recurring or non-recurring. **Yes** = recurring, **No** = non-recurring.
Scheduled	Indicates the date and time at which the job was scheduled to begin.
Component	Indicates the component in which the job originated; for example, **Investigation** or **Administration**.
Owner	Indicates the owner of the job. The owner of the job is not included in the default **Jobs Tray**, because only the current user's jobs are displayed here. The column is available to add.
Action	Views the job in another view or downloads job files for the job to the default **Downloads** directory on the local system. Only successfully completed jobs have the **View** link in the **Action** column. Only jobs that create a file have the **Download** link in the **Action** column.
Message	Displays additional information about the job; for example, **Extracting files** or **No sessions found.**
Query	Displays the query associated with the job to help you understand any issues with the result. This example provides the deviceid and the query that was submitted: `[Deviceid = 7 query = select * where sessionid=35667 size = 0 flags = 0]`
Status	Indicates the status of the job. Common values for status are **Paused**, **Running**, **Canceled**, **Failed**, **Completed**, and other status values are possible.
Progress	Shows the percentage complete for a job.
View Your Jobs	(Jobs tray only) Displays your jobs in the **Jobs panel**.