RSA NETWITNESS® PLATFORM

Getting Started Guide

for RSA NetWitness® Platform 11.5

Contact Information

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

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

September 2020

Contents

Getting Started with NetWitness Platform

Overview

RSA NetWitness® Platform is a powerful threat detection suite that enables Security Operation Centers (SOCs) to quickly locate, prioritize, and triage threats. NetWitness Platform 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 Platform 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

RSA NetWitness Platform is a distributed and modular system that enables highly flexible deployment architectures that scale with the needs of the organization. NetWitness Platform 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 Platform **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 RSA 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 Platform 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 Platform 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 Platform 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 Platform 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 Platform 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 Platform 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 Platform 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 Platform, 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 Platform supports modern (or current) versions of Google Chrome, Mozilla Firefox, 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 RSA NetWitness® Platform 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 Platform and internal users can log in to NetWitness Platform and receive role-based permissions. External user accounts authenticate outside of the NetWitness Platform and are mapped to NetWitness Platform roles. If you are an external user and you cannot access NetWitness Platform or view the information that you need, contact your System Administrator. Your Administrator can assign the appropriate roles to your account.

NetWitness Platform 11.4 or later 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: In 11.4 or later, 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.

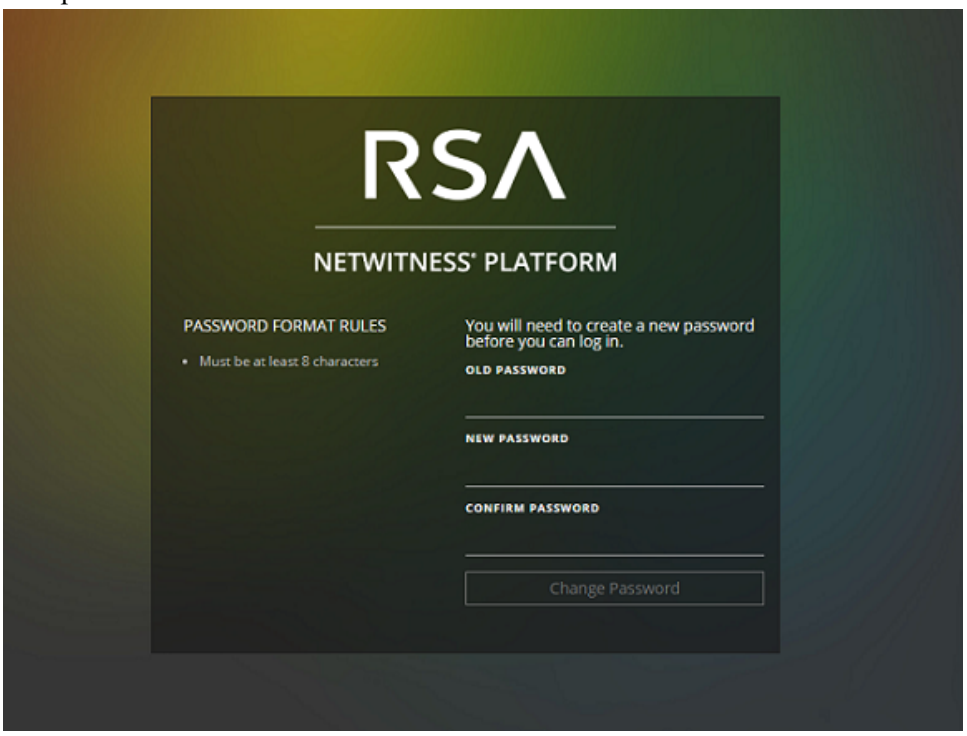
If you try too many times to log in with an incorrect username or password, your account will be locked. Contact your Administrator to unlock your account.

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 Platform:

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 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**.

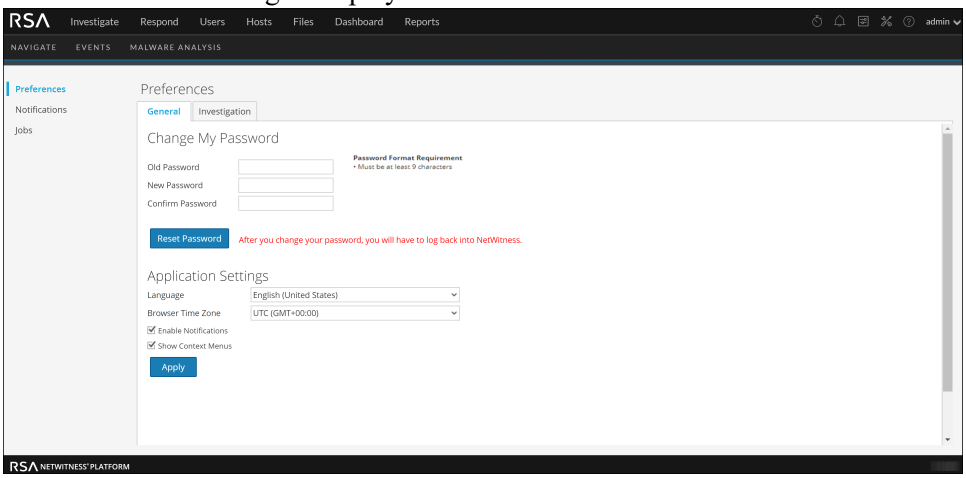
Changing Your Password

You can change the password that you use for RSA NetWitness® Platform authentication at any time in your user preferences. Your administrator defines the appropriate password strength requirements for your NetWitness Platform 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 Platform 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 Platform for the changes to take effect. The new password becomes effective the next time you log in to NetWitness Platform.

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 RSA NetWitness® Platform 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

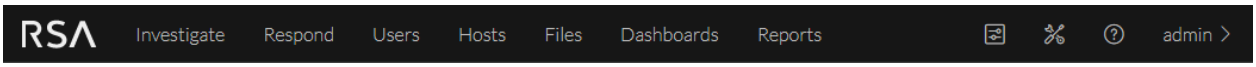
System Administrator

- 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 RSA NetWitness® Platform application is divided into ten main functional areas, known as views, that are based on typical Security Operation Center (SOC) roles.

Note: On upgrade to version 11.5 or later, by default the Springboard is displayed if you have not configured the default landing page in previous versions.



- **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 RSA 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 Platform 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 Platform 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 Platform. 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.

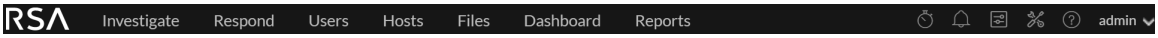
Menu changes

The following table illustrates the top-level menu changes in the 11.5 version.

Previous Version - 11.4 and earlier	11.5 Version
N/A	RSA Click the RSA logo at the top left corner to view the Springboard.
Monitor > Dashboard Monitor > Reports	Dashboard Reports
Investigate > Hosts Investigate > Files Investigate > Entities	Hosts Files Users
Configure	
Admin	

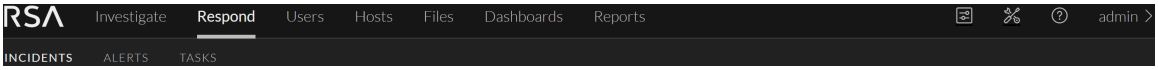
Accessing Main Views

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.



Secondary Menus

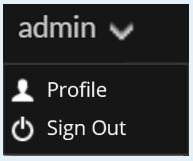
The main views have secondary menus with additional views that you can select, which vary according to the tasks that you can complete. The following example shows the Respond menu.



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 Platform 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 Platform.
	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 Platform UI.
	Help	Click this icon to view NetWitness Platform help topics.

Main Views

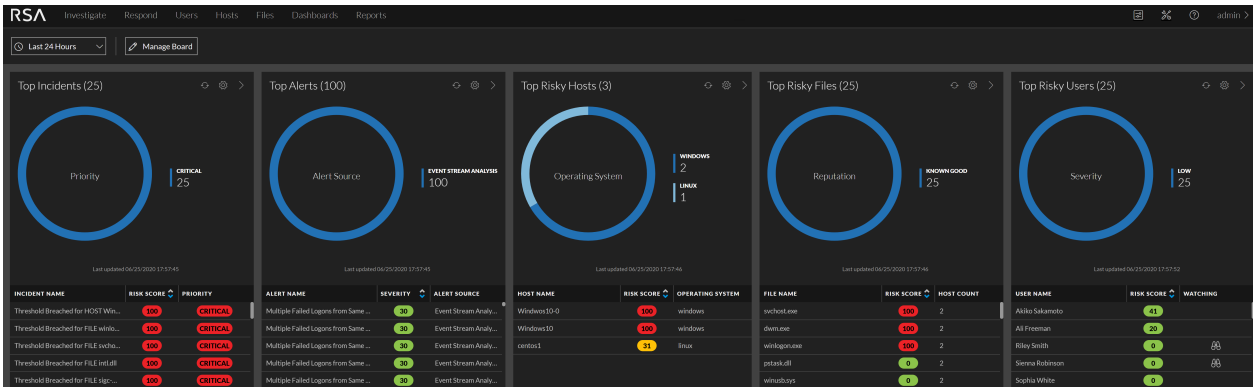
The following sections explain the main views:

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

Springboard

(From 11.5 and later) RSA 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 RSA logo at the top left corner to view the Springboard.



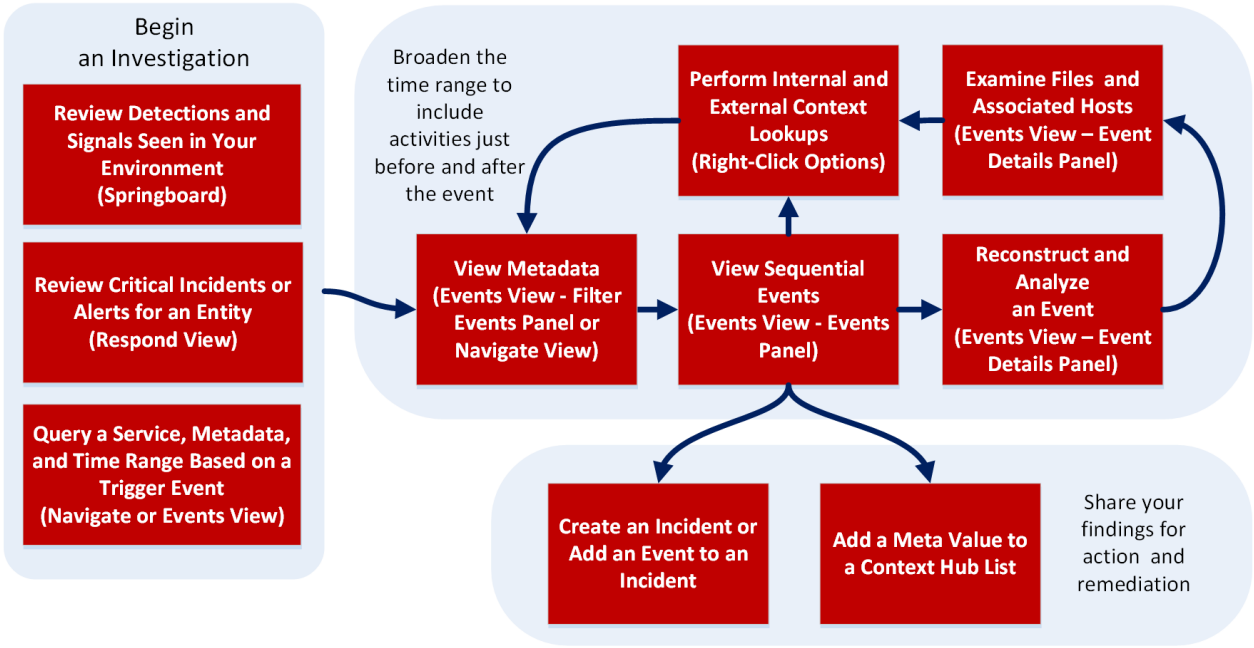
What can I do here?	Path	Show me how
View out-of-the-box panels Edit a panel Refresh a panel Select time range View all incidents, alerts, users, files, and hosts View details of selected incident, alert, user, file, and host Manage Board (add, rearrange, and delete panels)	Springboard view	See Managing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

Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

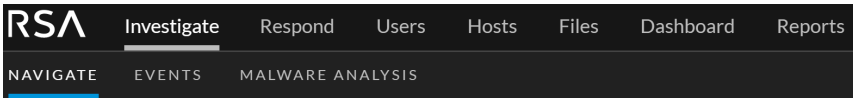
Investigate

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.

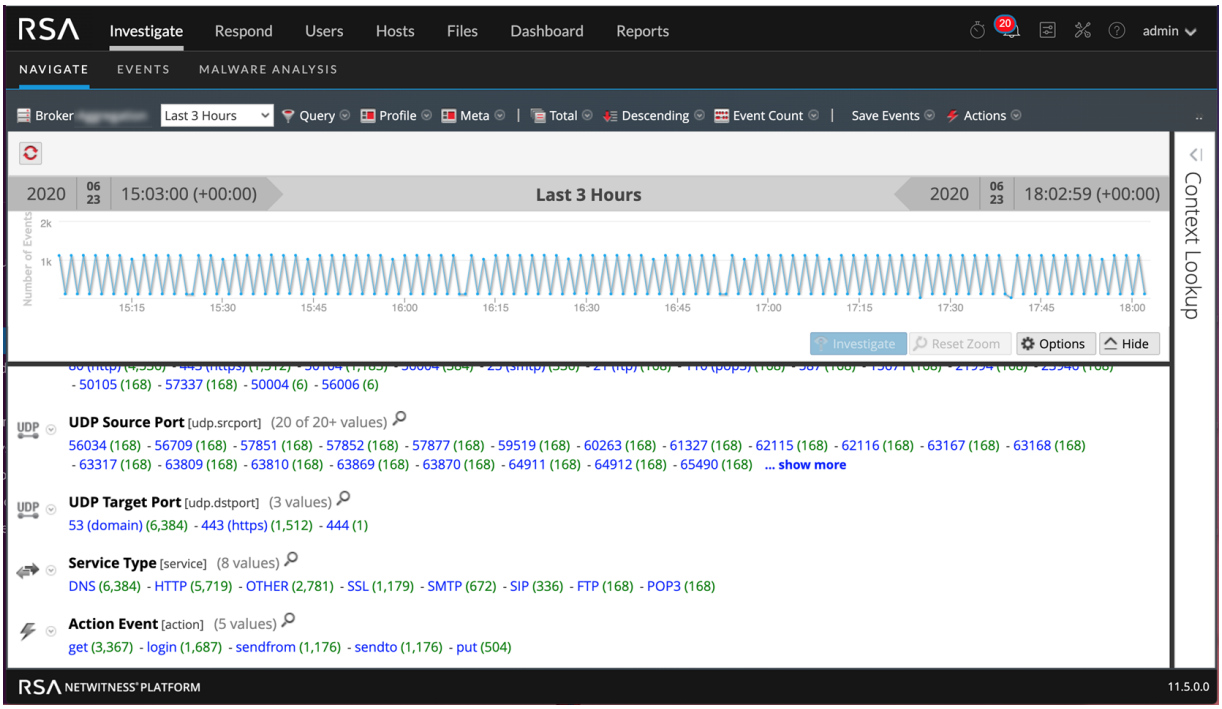


Investigate Menu

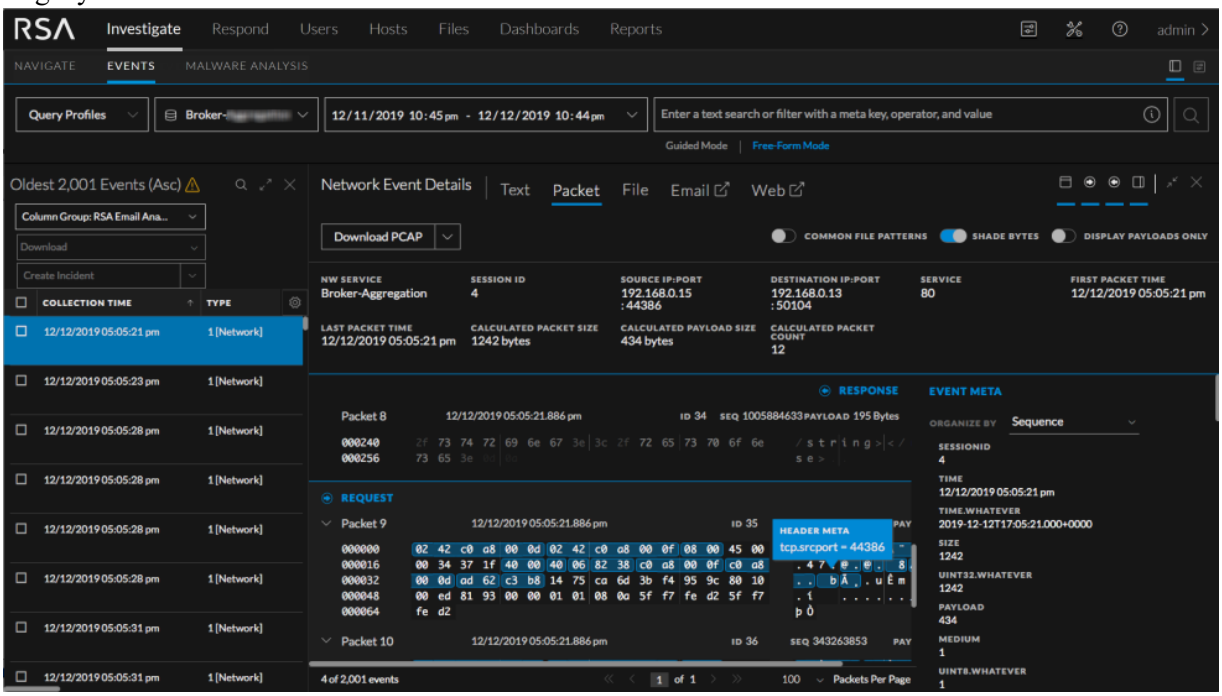


The Investigate menu has the following options:

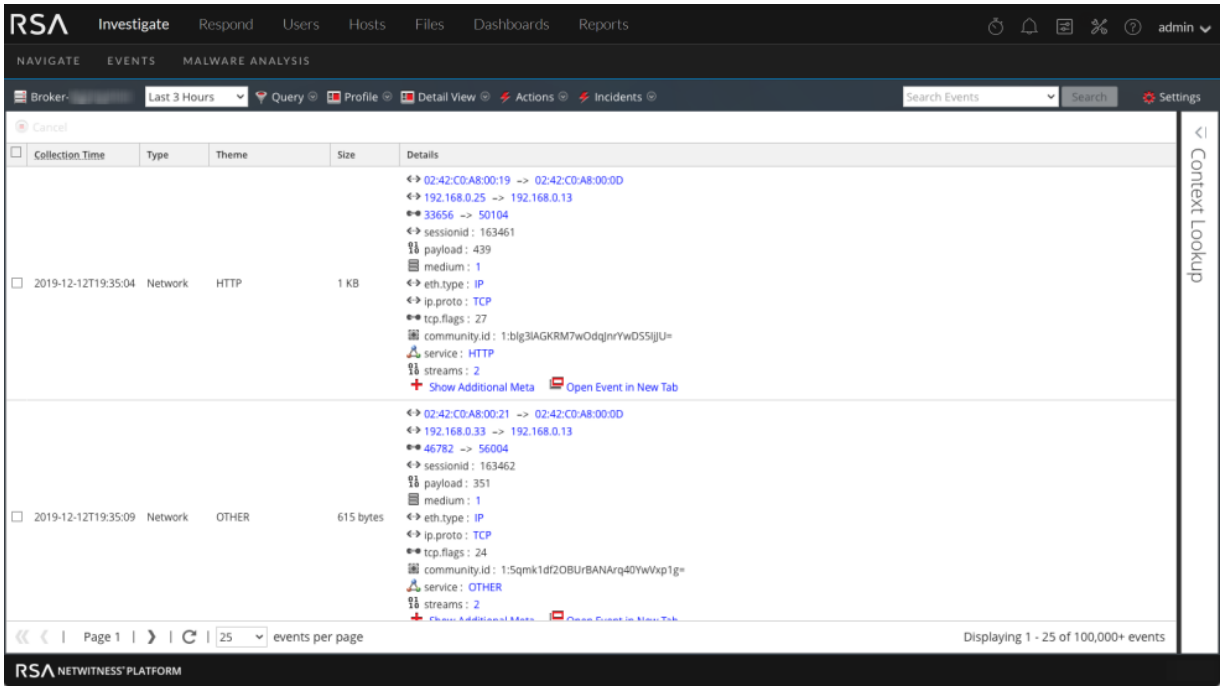
- **Navigate**: The Navigate view provides a list of meta keys and meta values with a focus on metadata. You can drill into the data, search for events, open a selected event in the Events view, and look up additional context from the Context Hub service.



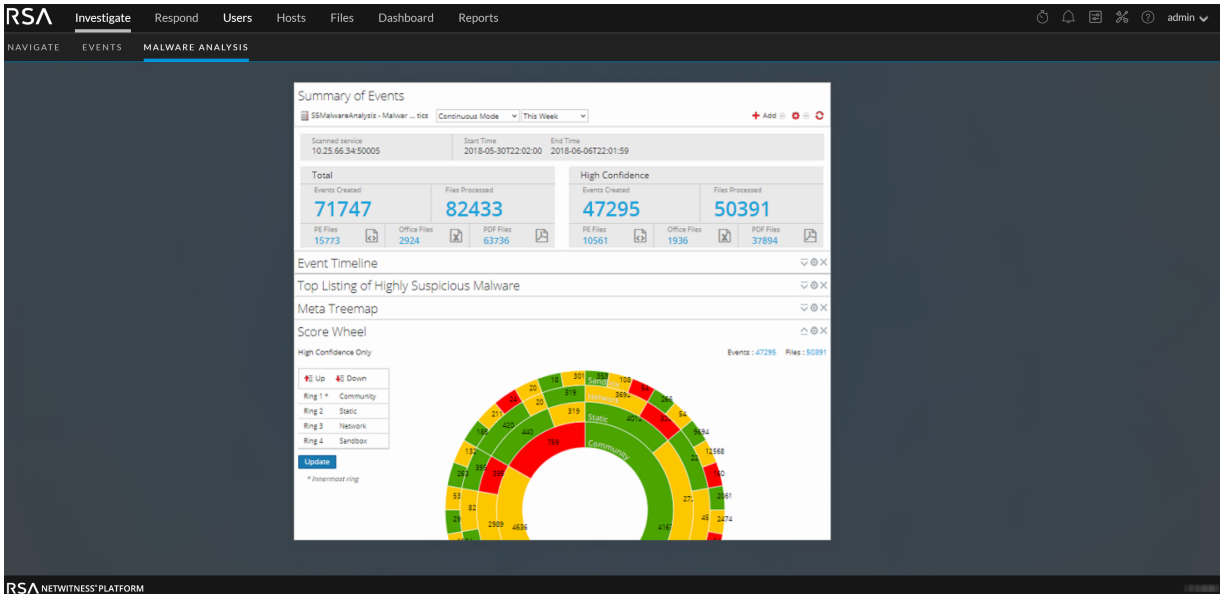
- **Events**: The Events view (formerly Event Analysis view) is the default user interface for interacting with events. It provides a sortable list of events with focus on metadata and raw data. You can search for events, view a reconstruction that offers helpful cues to identify points of interest, 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 11.3 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.



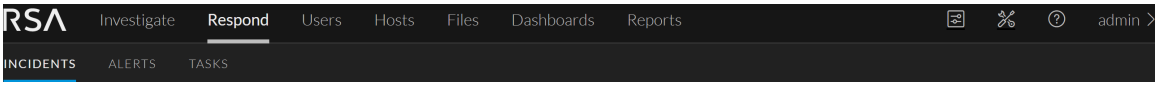
What can I do here?	Path	Show me how
Configure Investigate Views and Preferences	Investigate view	See "Configuring Investigate Views and Preferences" in the *NetWitness Investigate User Guide*.
Browse Event Metadata	Navigate view	See "Refining the Results Set" in the *NetWitness Investigate User Guide*.
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 Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

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.

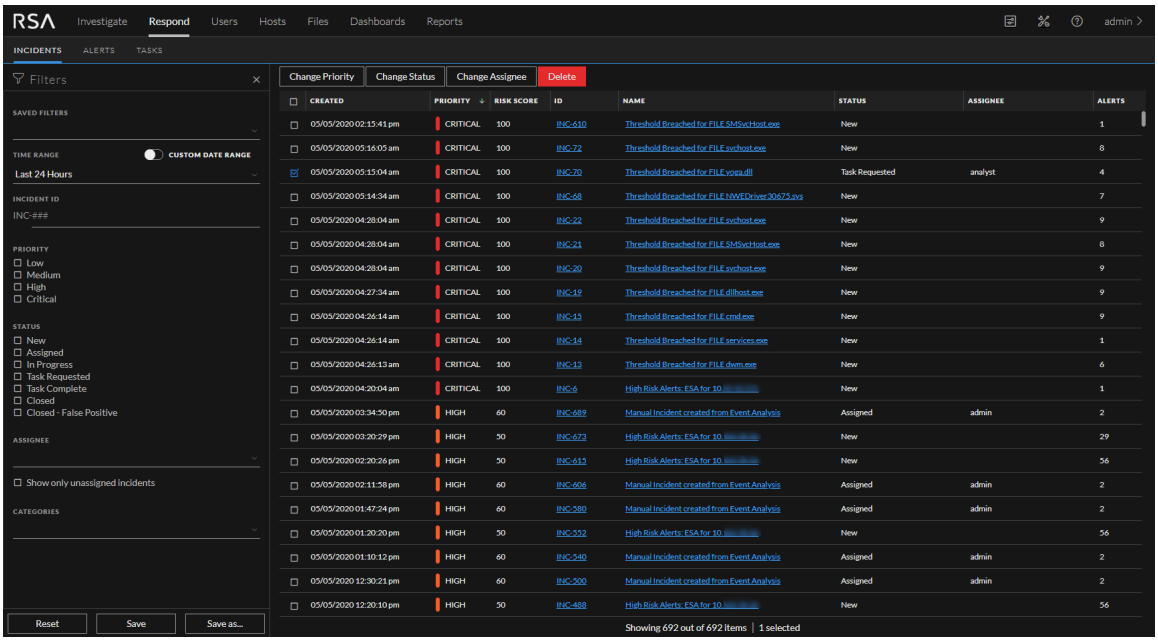
Respond Menu



The Respond menu has the following options:

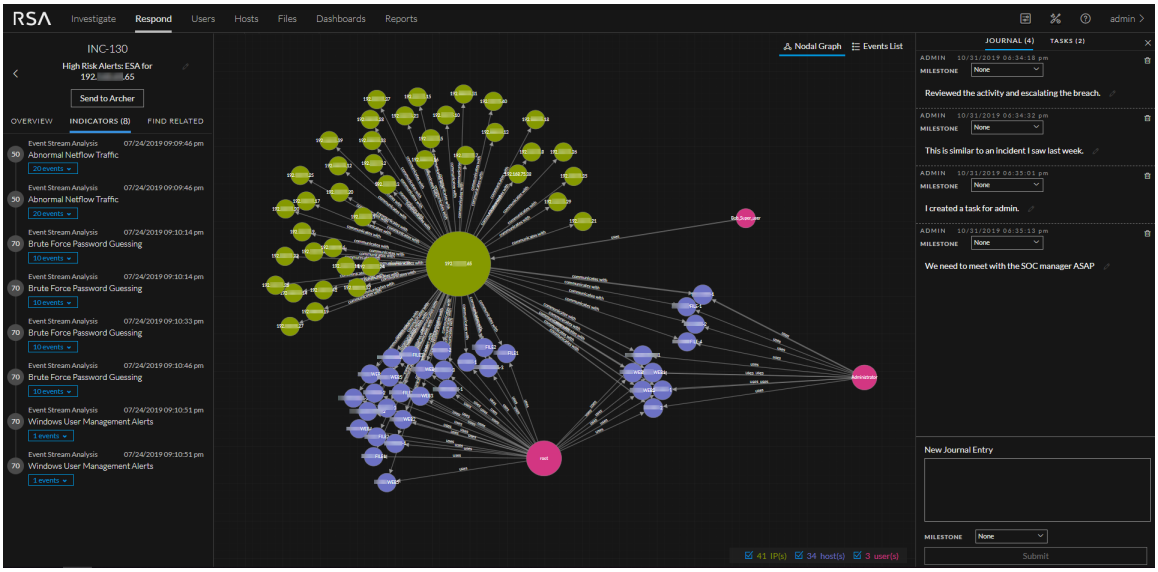
- **Incidents**: The Incidents List view contains a list of all incidents with basic information. The Incident Details view provides extensive details about the incident.
- **Alerts**: The Alerts List and Alert Details views provide information about all of the threat alerts and indicators received by NetWitness Platform in one location.
- **Tasks**: The Tasks List view enables you to create tasks and track them to completion.

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

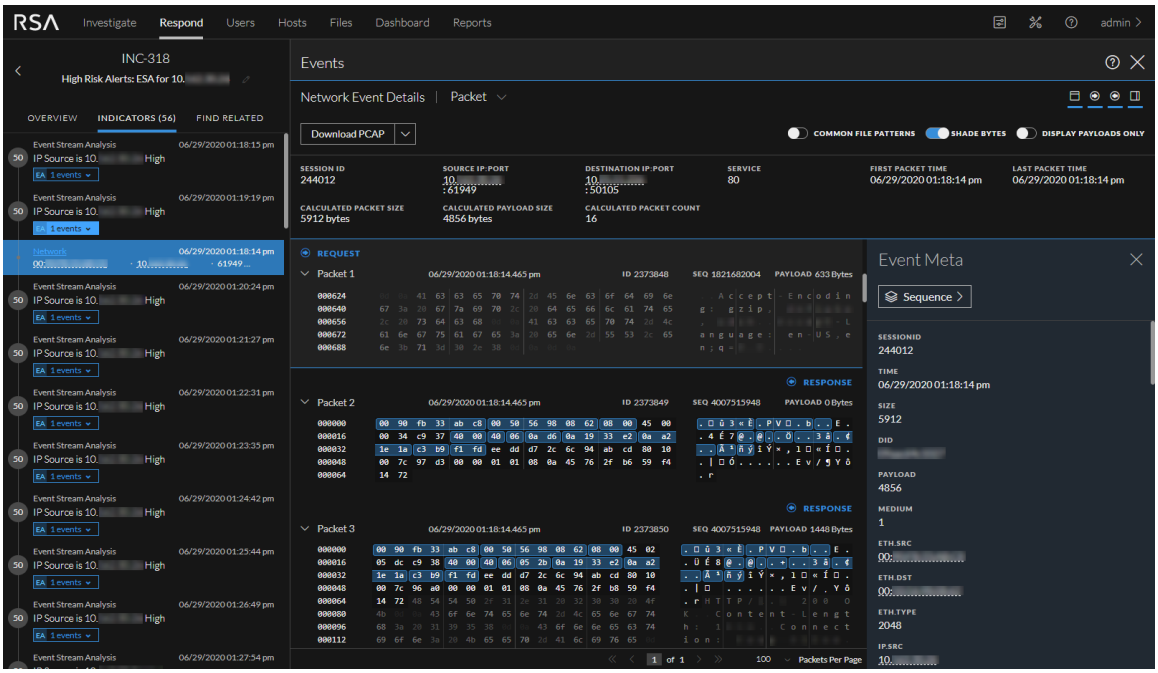


When using NetWitness Platform as your case management tool, you can also manage incidents from this view. New incidents appear at the top of the incident queue.

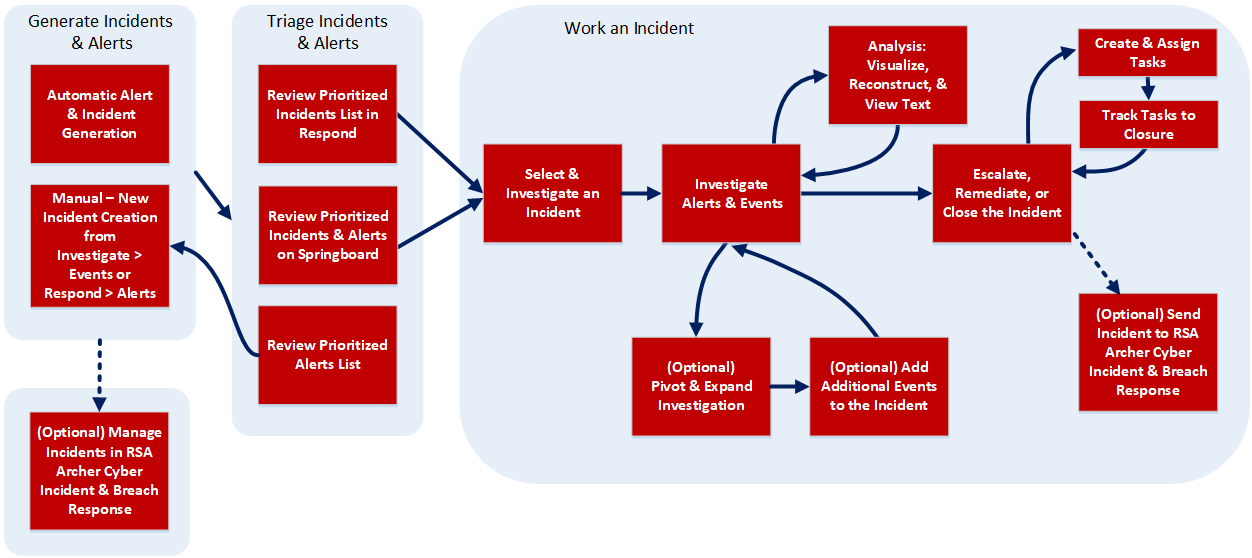
The following figure shows an example of the Respond view - Incident Details view, which shows details for a selected incident.



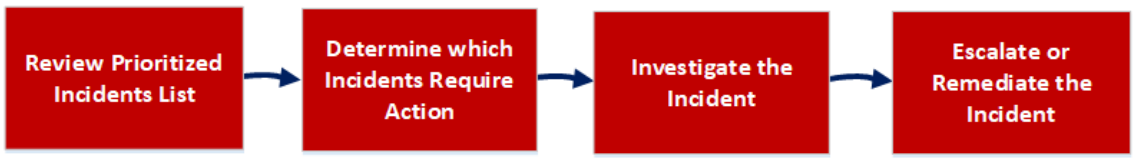
The Respond view is designed to make it easy to evaluate incidents, contextualize that data, collaborate with other analysts, and pivot to a deep-dive investigation as needed. The following figure shows an example of an event analysis in the Incident Details view.



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.



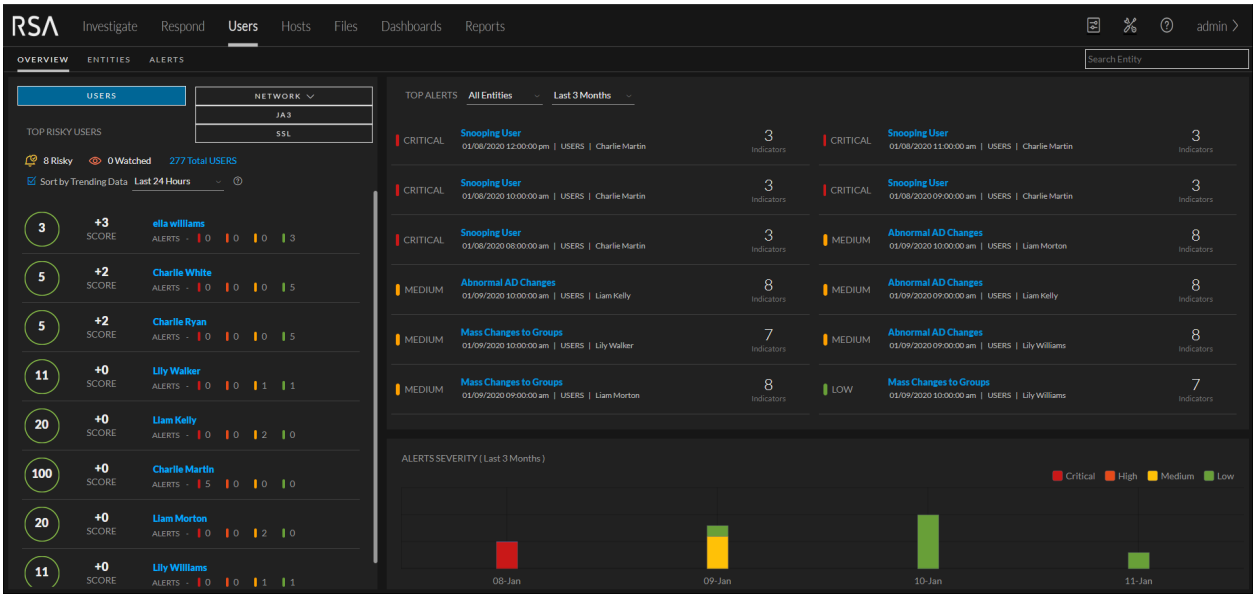
In the Respond view, analysts look at the prioritized list of incidents and determine which incidents require action. They click an incident for a clear picture of the incident with supporting details and they can investigate the incident further. Analysts can then determine how to respond to the threat, 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 Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Users

The Users view provides visibility into risky user behaviors across your enterprise with RSA 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.

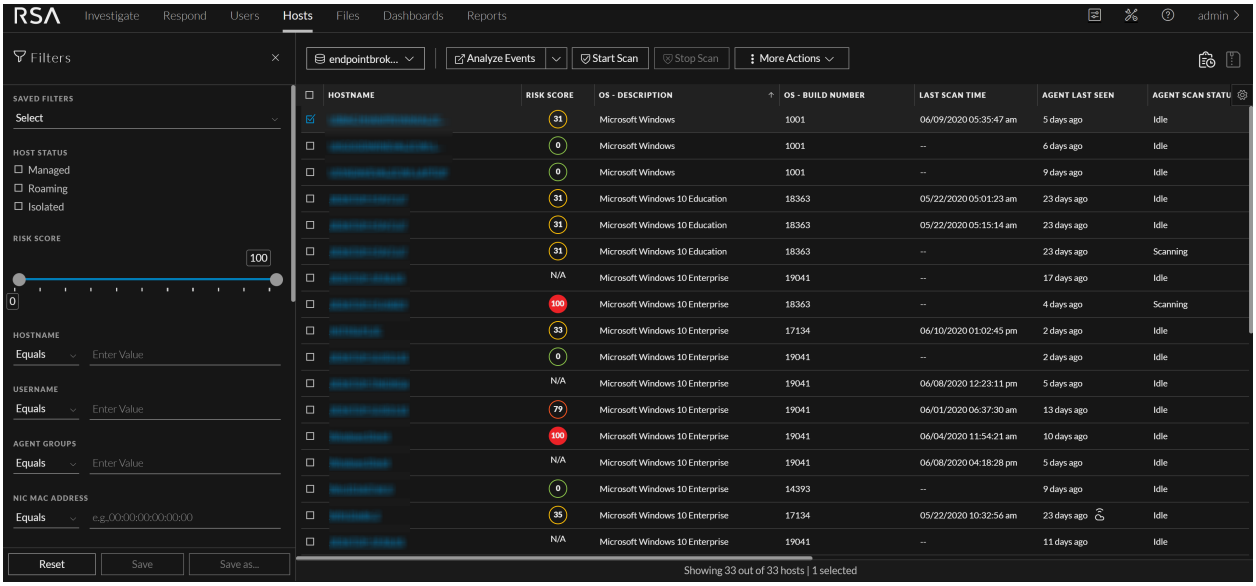
- **Alerts**: It displays details about all the alerts in your environment. You can view forensic information about suspicious activity in your environment that is based on a specific timeframe.

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

Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

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.

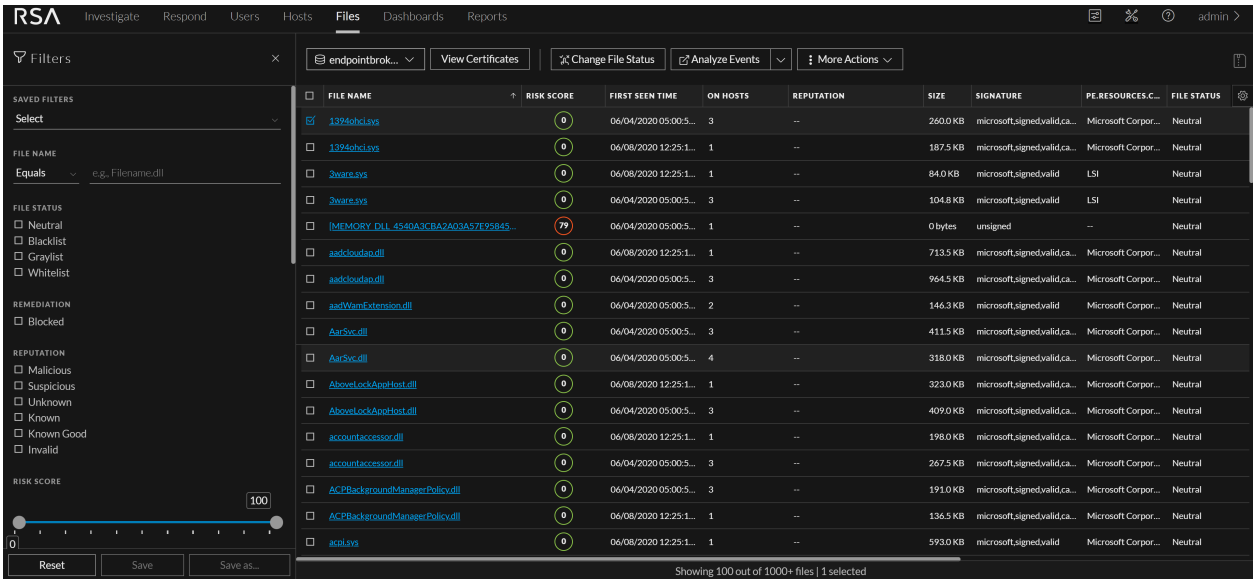


What can I do here?	Path	Show me how
Investigate Endpoints	Hosts view	See the *NetWitness Endpoint User Guide*.

Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

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.

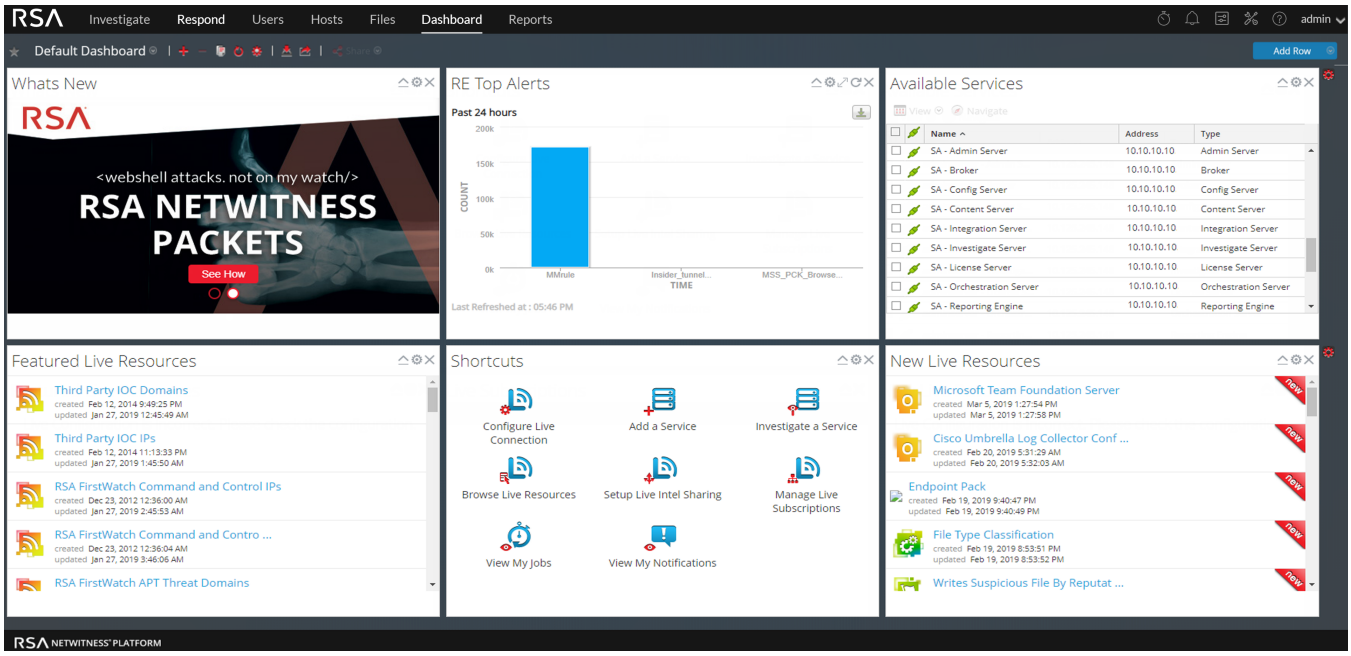


What can I do here?	Path	Show me how
Find Suspicious Endpoint Files	Files view	See the *NetWitness Endpoint User Guide*.

Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

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 RSA 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

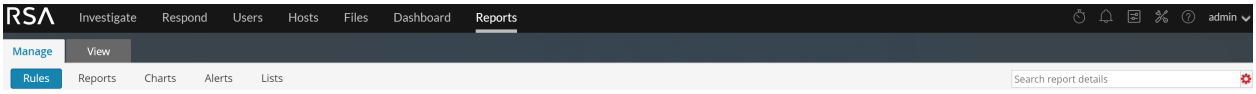
What can I do here?	Path	Show me how
Select a Dashboard	Dashboard view	See Managing Dashboards.
Create a Dashboard	Dashboard view	See Managing Dashboards.
Manage Dashboards	Dashboard view	See Managing Dashboards.

Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

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.

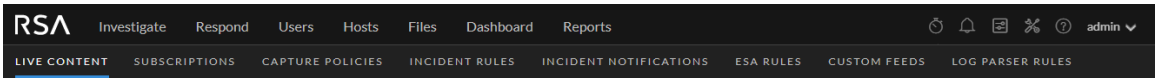
What can I do here?	Path	Show me how
View a Report	Reports > View	See the *Reporting User Guide*.
Manage Reports	Reports > Manage	See the *Reporting User Guide*.

Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Configure

The Configure view enables Threat Intel personnel (Content Experts) to configure data sources and inputs to NetWitness Platform 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 Platform that manages communication and synchronization between NetWitness Platform services and a library of Live content available to RSA NetWitness Platform customers. You can view, search, deploy, and subscribe to content from the RSA Live Content Management System (CMS) to NetWitness Platform 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 Platform, you configure the connection and synchronize between the CMS server and NetWitness Platform.
- **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.
- **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 Platform 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.

  Note: The Log Parser Rules tab is available in the Configure menu in versions 11.2 and later. For earlier versions, it is located in Admin > Event Sources.

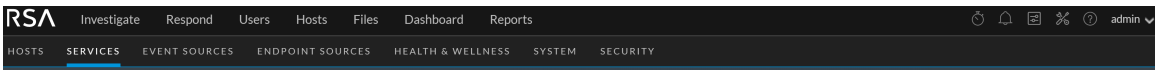
What can I do here?	Path	Show me how
Create a Live Services account.	RSA Live Registration Portal: https://cms.netwitness.com/registration/	See the *Live Services Management Guide*.
Find and deploy Live Services resources.	(Configure) > Live Content	See the *Live Services Management Guide*.
Set up selective network data collection.	(Configure) > Capture Policies	See the *Decoder Configuration Guide*.
Set up Live Services Services on NetWitness Platform.	(Configure) > Subscriptions	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*.

Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Admin

In the Admin view, administrators can manage network hosts and services; monitor the health and wellness of NetWitness Platform; 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 Platform hosts and services in your network environment.
- **System**: The System view enables you to set global NetWitness Platform 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 Platform 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 Platform roles, and modify other security-related system parameters. These apply to the NetWitness Platform system and are used in conjunction with the security settings for individual services.

Note: For versions 11.2 and later, the Event Sources > Log Parser Rules tab can be found in the Configure view.

What can I do here?	Path	Show me how
Manage hosts.	(Admin) > Hosts	See the *Host and Services Getting Started Guide*.
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 Platform domain.	(Admin) > Health & Wellness > Alarm	See the *System Maintenance Guide*.

What can I do here?	Path	Show me how
Monitor statistics for the NetWitness Platform 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 Platform domain.	(Admin) > Health & Wellness > Policies	See the *System Maintenance Guide*.
Set global configurations for NetWitness Platform.	(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 Platform 11.3 and later.	(Admin) > Security	See the *System Security and User Management Guide*.

Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Setting Up Your Default View by SOC Role

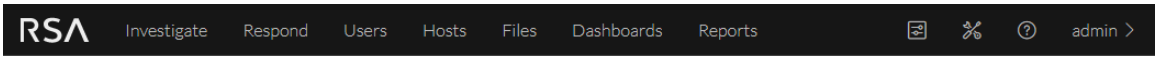
After logging in to RSA NetWitness® Platform, you can navigate into the application easier by setting up your default view based on your Security Operations (SOC) role. You can set your default view, also known as a landing page, in your user preferences.

On upgrade to version 11.5 or later, by default the Springboard is displayed if you have not configured the default landing page in previous versions.

In version 11.4 and prior versions, if you configured the default landing page as Respond or Investigate in the User Preferences, then on upgrade to version 11.5, the default landing page will be Respond or Investigate view.

On fresh install of RSA NetWitness® Platform 11.5 version, when you log in, by default Springboard is the landing page.

The following figure shows the main NetWitness Platform views.



- **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 Platform. 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 Platform views as your default view. In addition to the main views, NetWitness Platform 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

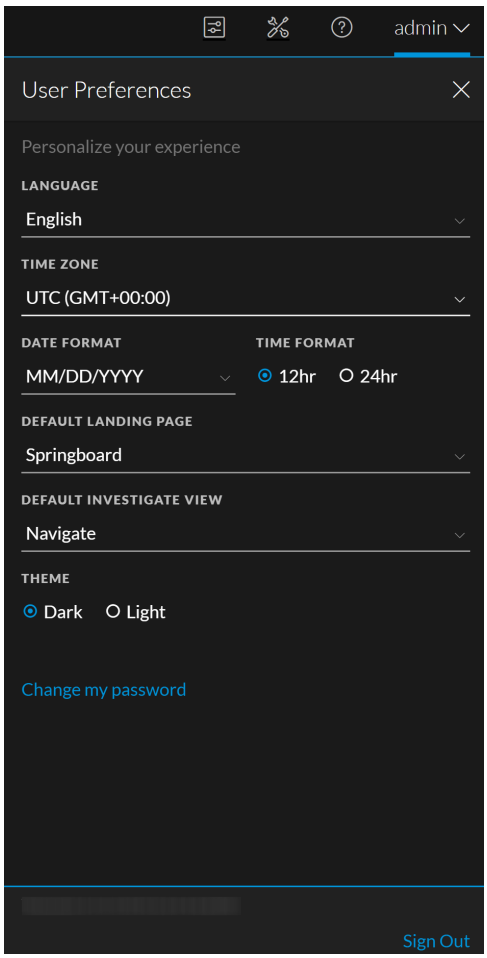
The following table shows typical SOC roles and the available views you can select as your landing page in your user preferences based on your SOC role. If you have more than one role, select the view that is most appropriate for you to start with when you log in to NetWitness Platform.

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 Platform.	**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.
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, admin.

   The User Preferences dialog shows your current preferences.



2. In the **Default Landing Page** field, select the default view that you would like to see when you log in to NetWitness Platform. 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.

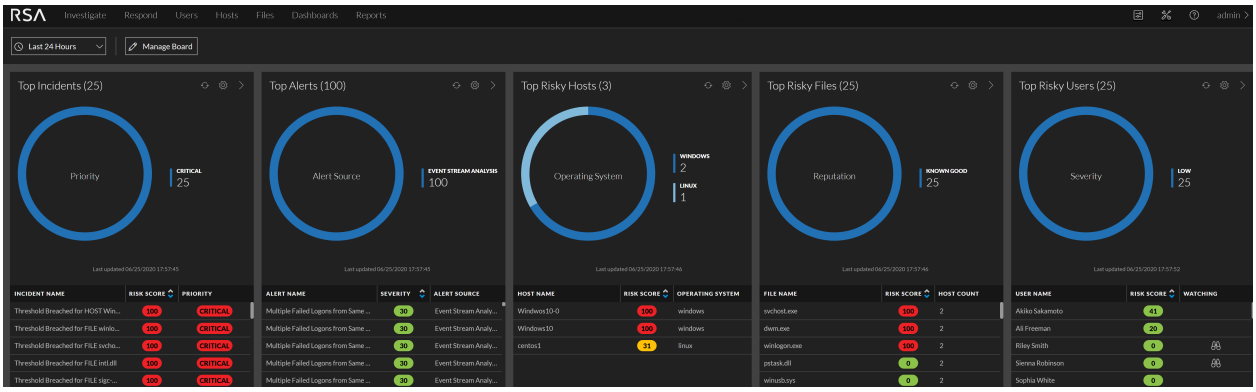
3. To verify that you can see the correct default view, click **Sign Out** to log out and then log back in to NetWitness Platform.

Managing the Springboard

(From 11.5 and later) RSA NetWitness Platform Springboard presents platform-wide detections and signals in this view so analysts hunt and investigate faster than ever before.

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.



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

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.

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.
- 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 **Respond > Incidents** list view.

- Scroll to view the different panels using the scroll bar available below the panels.

Administrators can customize the Springboard by performing the following:

- 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.

Add a Panel

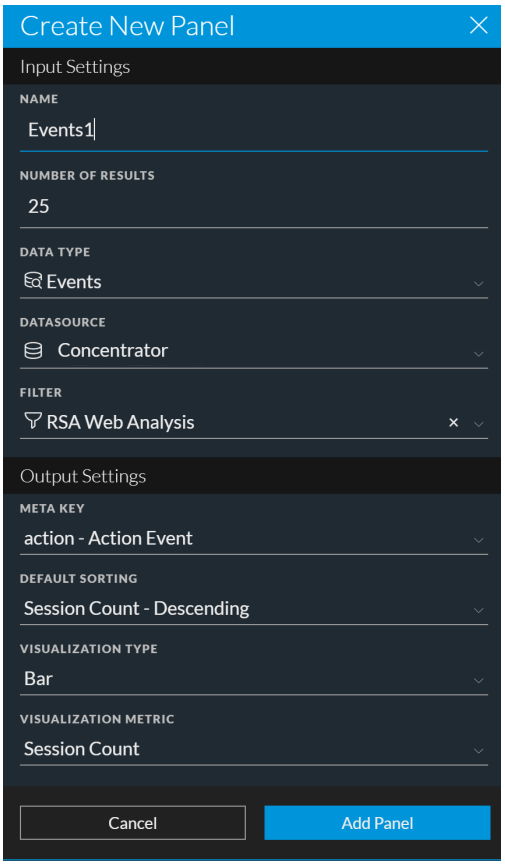
You can add a panel to the Springboard according to the analyst preferences. For example, an analyst can watch top risky users or top risky hosts for a particular region in a panel.

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

To add a panel:

1. Click **Manage Board**.
2. Click + New Panel 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
   - **Data Source**: Select the source of the data to use for the panel. This field is enabled when the data type is Events, Files, or Hosts.
     - Events: Select either Broker or Concentrator.
     - Files: Select either Endpoint Broker Server or Endpoint Server.

- Hosts: Select either Endpoint Broker Server or Endpoint Server.

- (Optional) **Filter** : Filter the data as required 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 RSA 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.

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

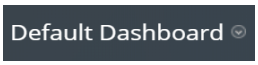
You can view dashboards on different areas of interest depending on your user permissions. You have the option to select a preconfigured dashboard, import a dashboard, or create your own custom dashboard. The dashboards help you to quickly and easily view reports. You can configure your dashboards to 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 Platform, 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 Platform 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 Platform 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.
+	Displays the Create a Dashboard dialog, where you define or add a custom dashboard.
−	Deletes a custom dashboard. The default dashboard cannot be deleted.

Option	Description
	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 Platform, 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:

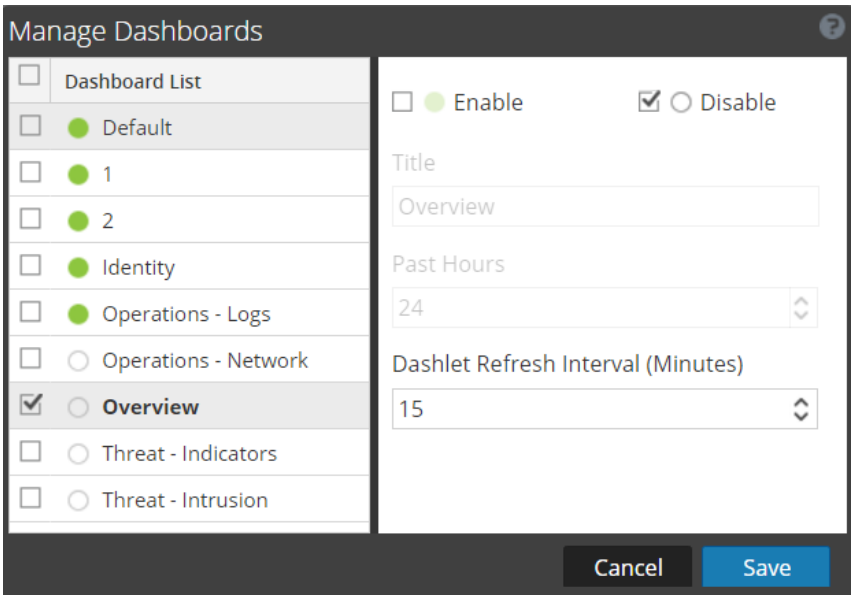
- Edit a dashboard
- Export a dashboard
- Share a dashboard
- Delete a dashboard

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

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

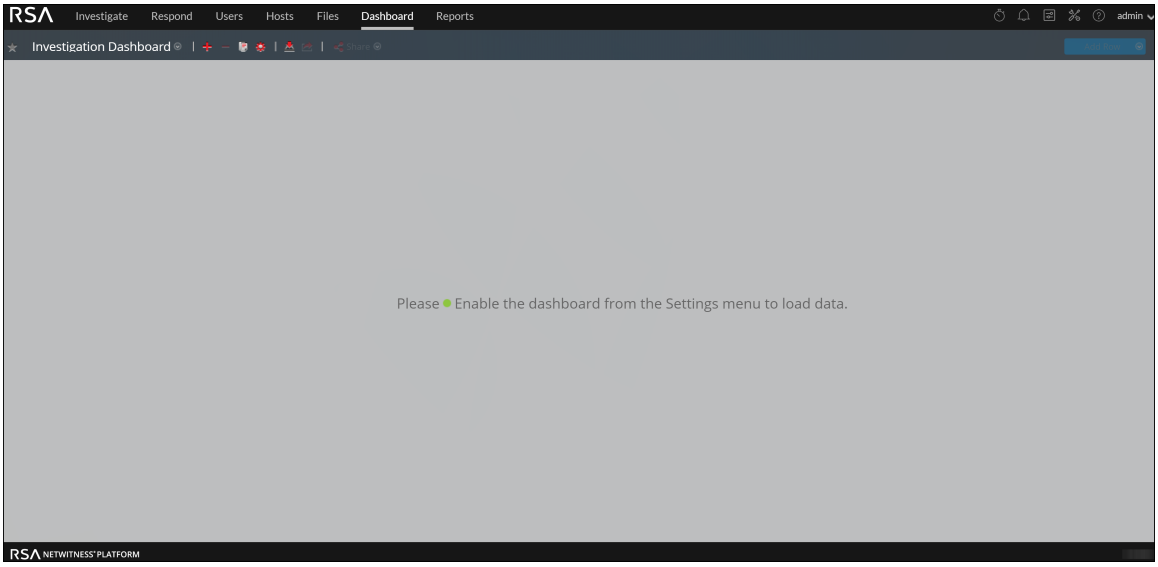


Name	Description
Dashboard List	Displays a list of the default, preconfigured, and custom dashboards.
Enable	Indicates if the selected dashlet is enabled.

Name	Description
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.

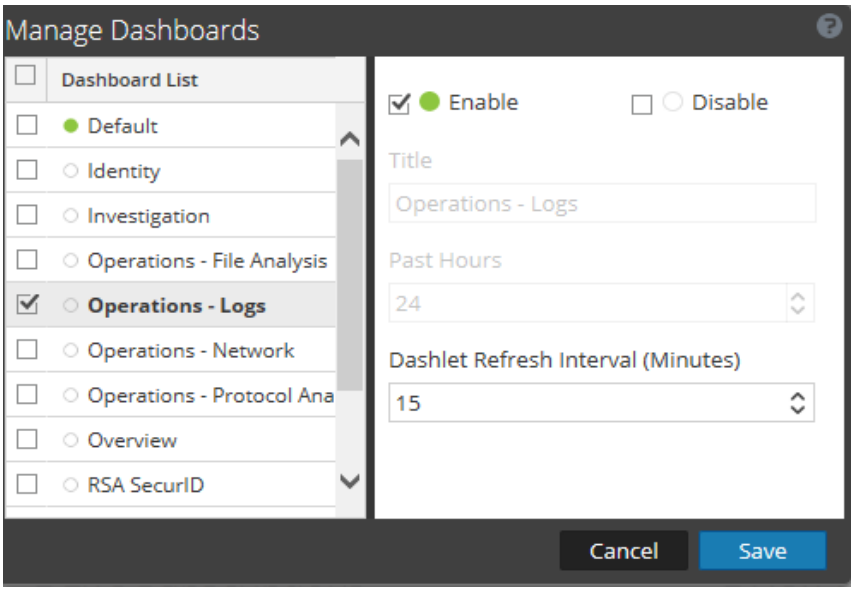
Enable a Dashboard

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.

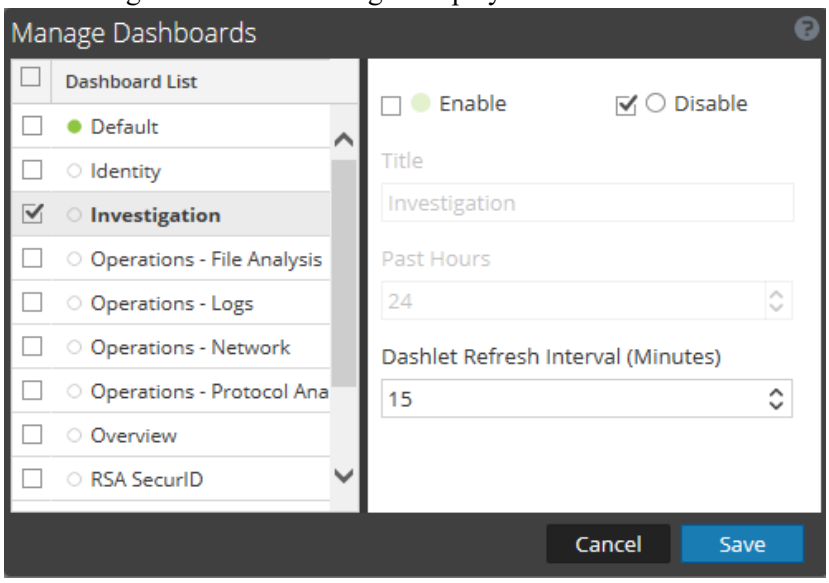


3. From the dashboard list, select the dashboards to be enabled.
4. Select the **Enable** checkbox.
5. Click **Save**.

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

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

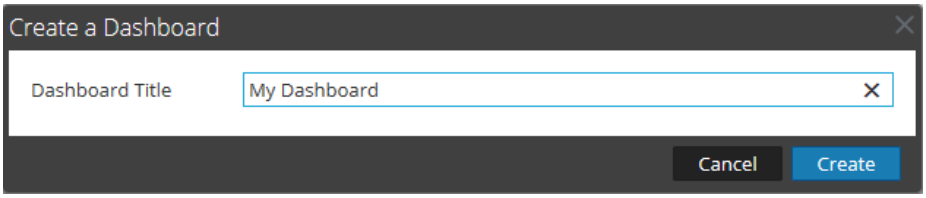
   If the favorite icon is red in color, it indicates that selected dashboard is set as a Favorite and is listed on top above the line.

Creating Custom Dashboards

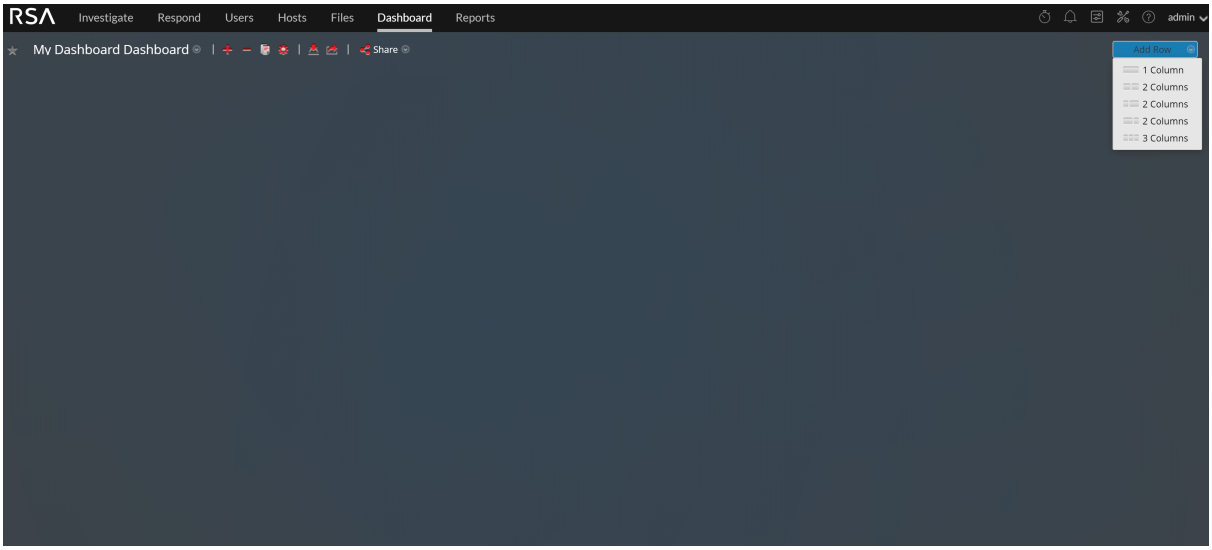
You can create custom dashboards to serve a particular purpose; for example, to represent a specific geographical or functional area of the network. Each custom dashboard is appended to the dashboard selection list.

To create a custom dashboard:

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

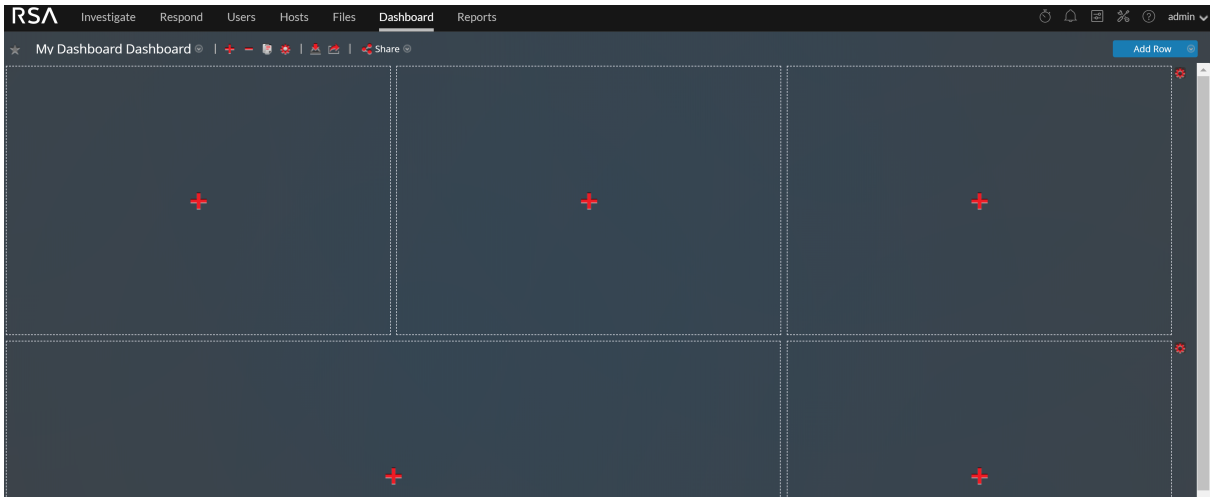


2. Enter a title for the new dashboard and click **Create**.
   The new dashboard is displayed as a blank screen.



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.

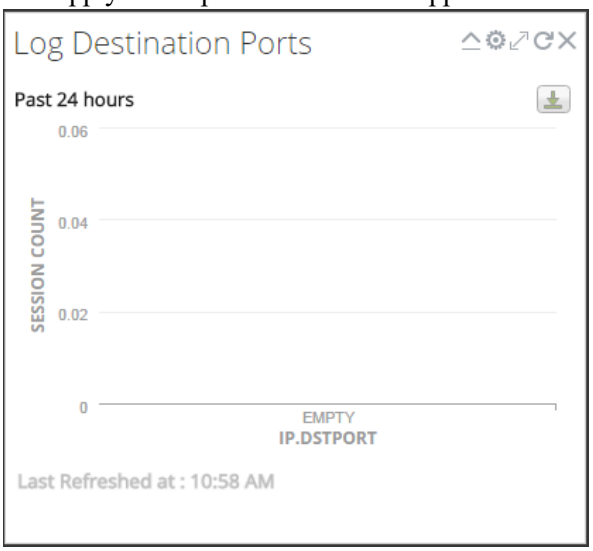
Each dashboard has:

- 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 Platform 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.
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.

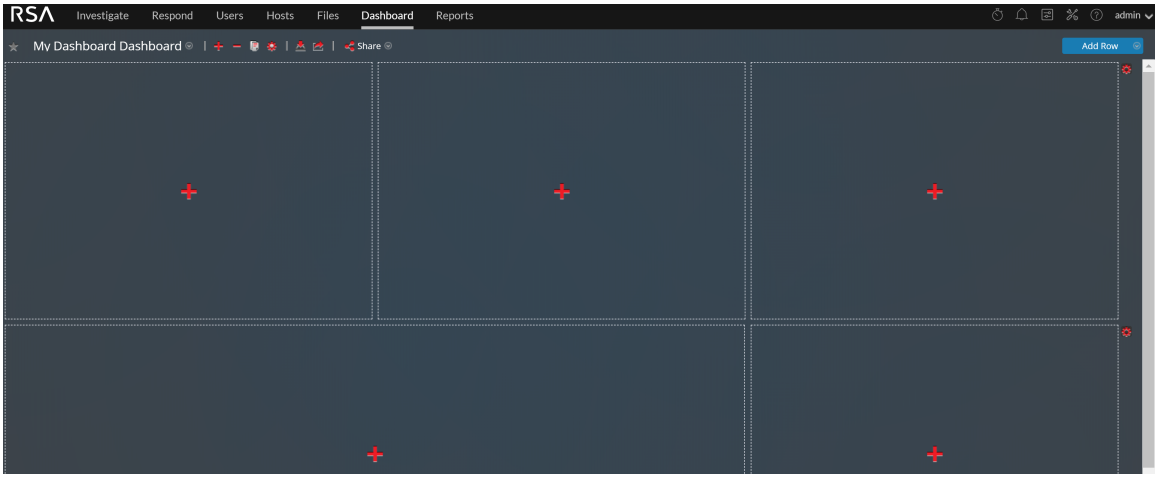
You can add dashlets to the default dashboard or construct a custom dashboard with your own useful set of dashlets to make your workflow more efficient.

Add a Dashlet

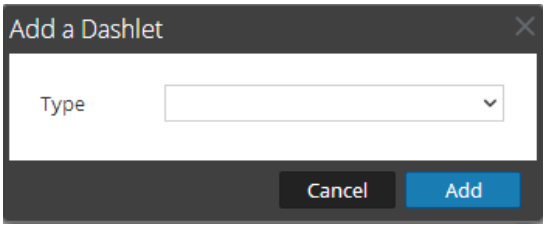
To customize the views in NetWitness Platform, you can add dashlets to a default dashboard or create custom dashboards. However, you cannot add dashlets to preconfigured dashboards.

To add a dashlet:

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

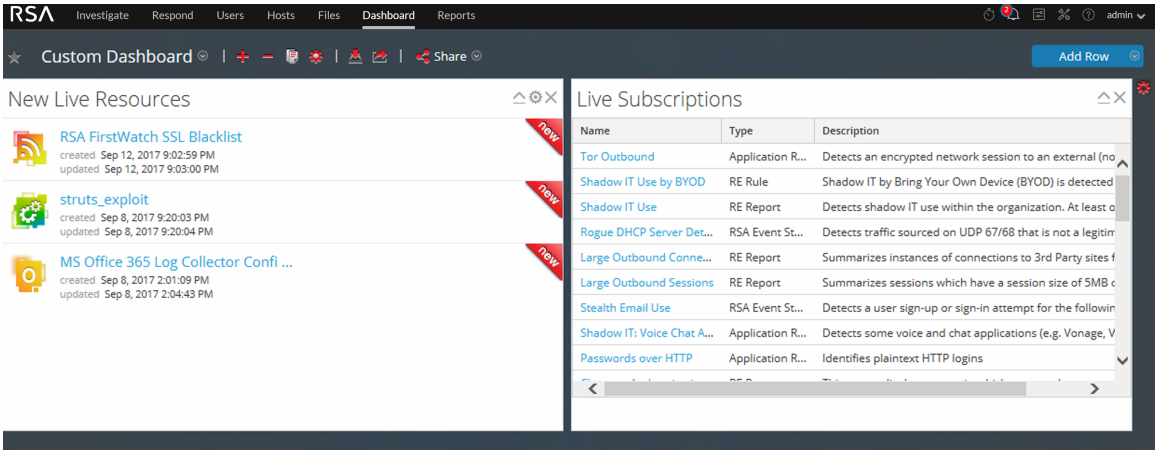


2. Click  on the placeholder where you want to add the dashlet.
   The Add a Dashlet dialog is displayed.



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.

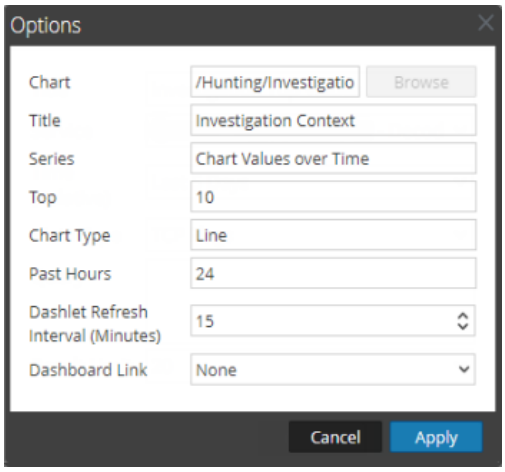
After the dashlets are added, you can drag and drop them and they can be swapped.

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.

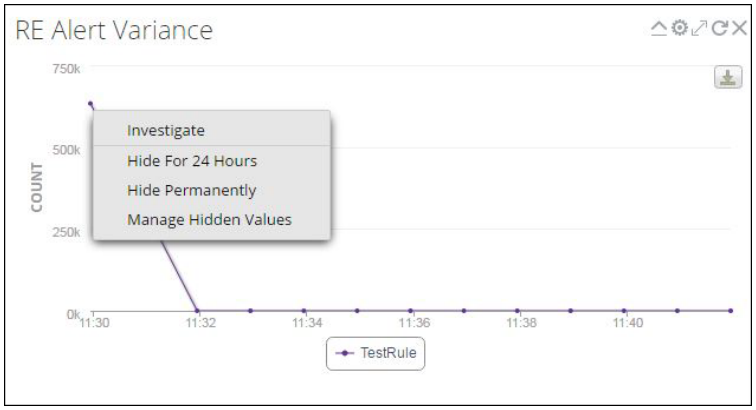
1. To display and modify the options for a dashlet, click settings (⚙) in the dashlet title bar.
   The Options dialog is displayed.



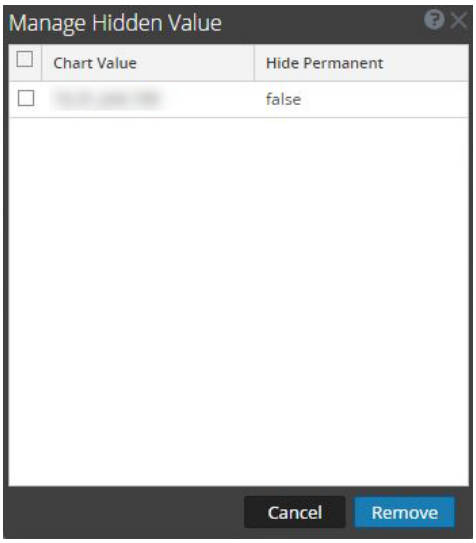
2. Edit any of the displayed properties. For example, in an in Operations - File Analysis Dashboard, edit Dashlet Refresh Interval from 15 to 20.
3. Click **Apply**.

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.

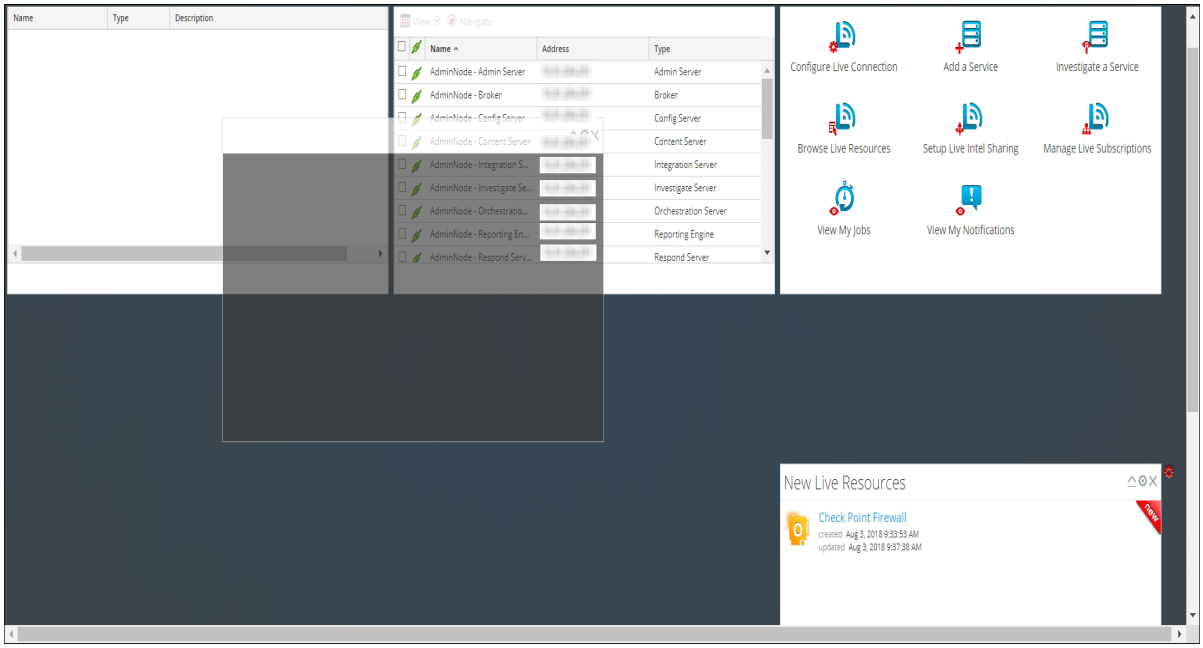
For more information on available dashlets, see the Dashboards Catalog in the RSA Content space on RSA Link.

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.



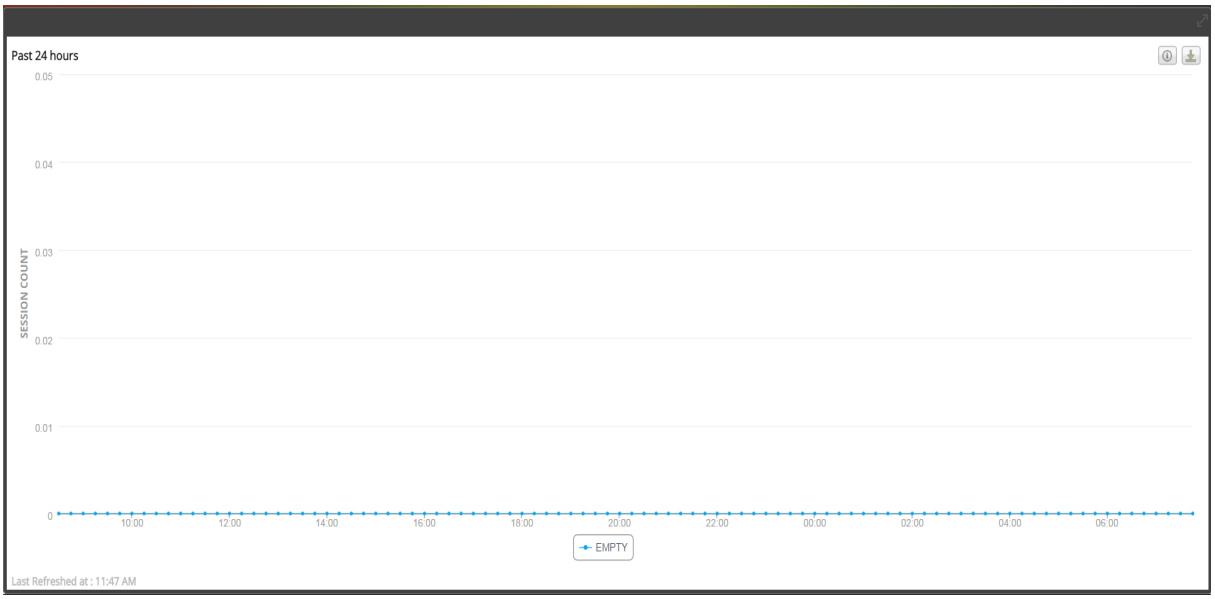
3. Release the mouse button when the dashlet is in the desired location.
   The dashlet that currently occupies that position moves down.

Maximize a Single Dashlet

This section explains how to open a dashlet on the entire area of the main NetWitness Platform 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.

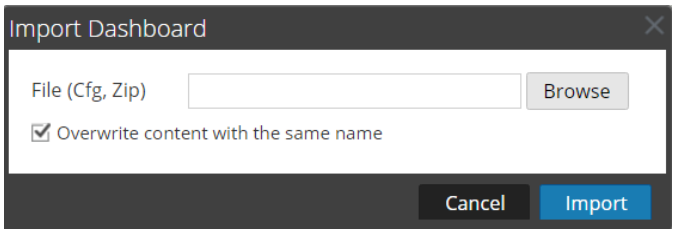
Note: After you remove the dashlet, the empty space is replaced by a placeholder where you can add another dashlet using the above Add a Dashlet procedure.

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 Platform.

Import a Dashboard

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 Platform

Note: If you import a dashboard from Security Analytics 10.6. x into NetWitness Platform11.x, the dashboard and the associated rules and charts must be imported separately. But when you import a dashboard from NetWitness Platform11.x into NetWitness Platform, the dashboard and all the rules and charts associated with it are imported in .zip format.

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 Platform 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.

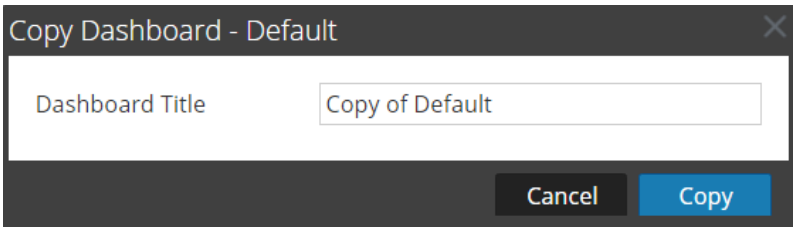
Note: The Export feature is not applicable for preconfigured dashboards.

Copying a Dashboard

To customize the views in NetWitness Platform, you can copy dashboards to the NetWitness dashboard or a custom dashboard. The NetWitness Platform dashboard, as the name suggests, offers all NetWitness Platform 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 Platform, 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  .

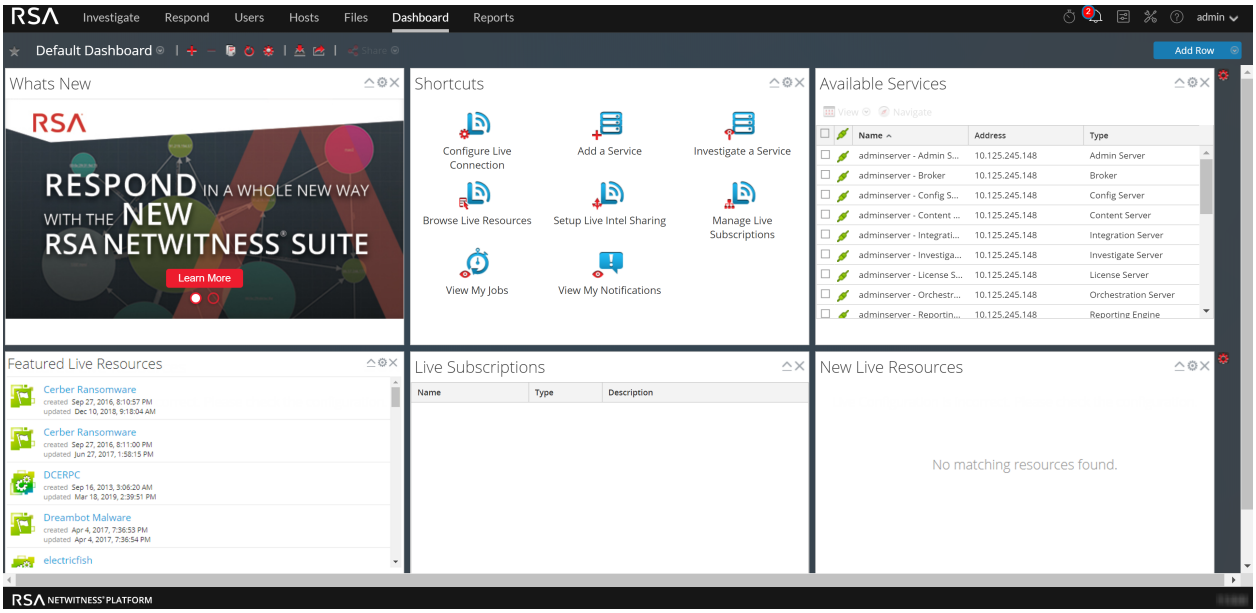
Using Dashboards in the Analyst User Interface

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 RSA NetWitness® Platform 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 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 Platform 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:

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.

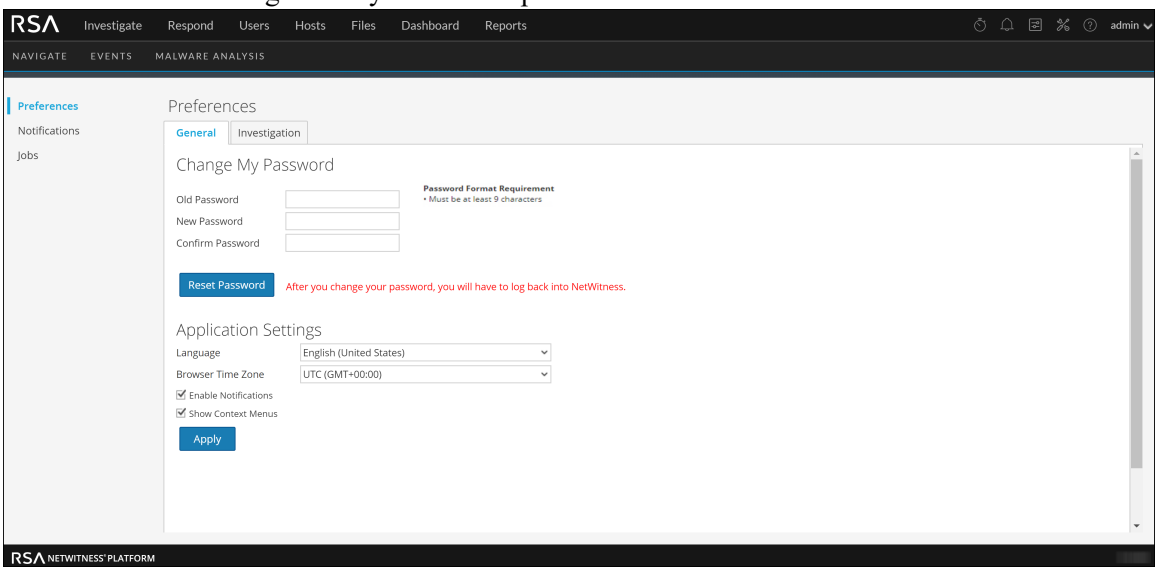
** You can make this change from the **Preferences** dialog accessible from these views: Investigate, Dashboard, Reports,  (Configure) > (Live Content, Subscriptions, ESA Rules, and Custom Feeds), and Admin. See Preferences.

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 Platform browser window, select your username, for example admin, and then select **Profile**.
The Preferences dialog shows your current preferences.



Set the Language and Time Zone

Note: The Language preference option applies to NetWitness Platform 11.2 and later.

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 Platform.
   b. **Browser Time Zone**: Set the time zone to use in the NetWitness Platform.
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 Platform 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*.

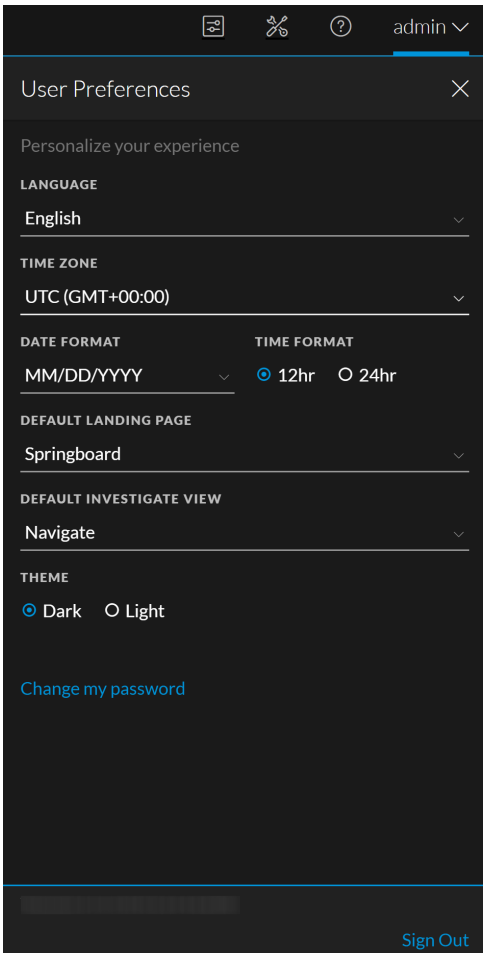
User Preferences

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 Platform browser window, select your username, for example, 

.
The User Preferences dialog shows your current preferences when accessed through the 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

Note: The Language preference option applies to NetWitness Platform 11.2 and later.

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 Platform.
   b. **Time Zone**: Set the time zone to use in the NetWitness Platform.
   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 Platform. You can choose 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 Platform 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

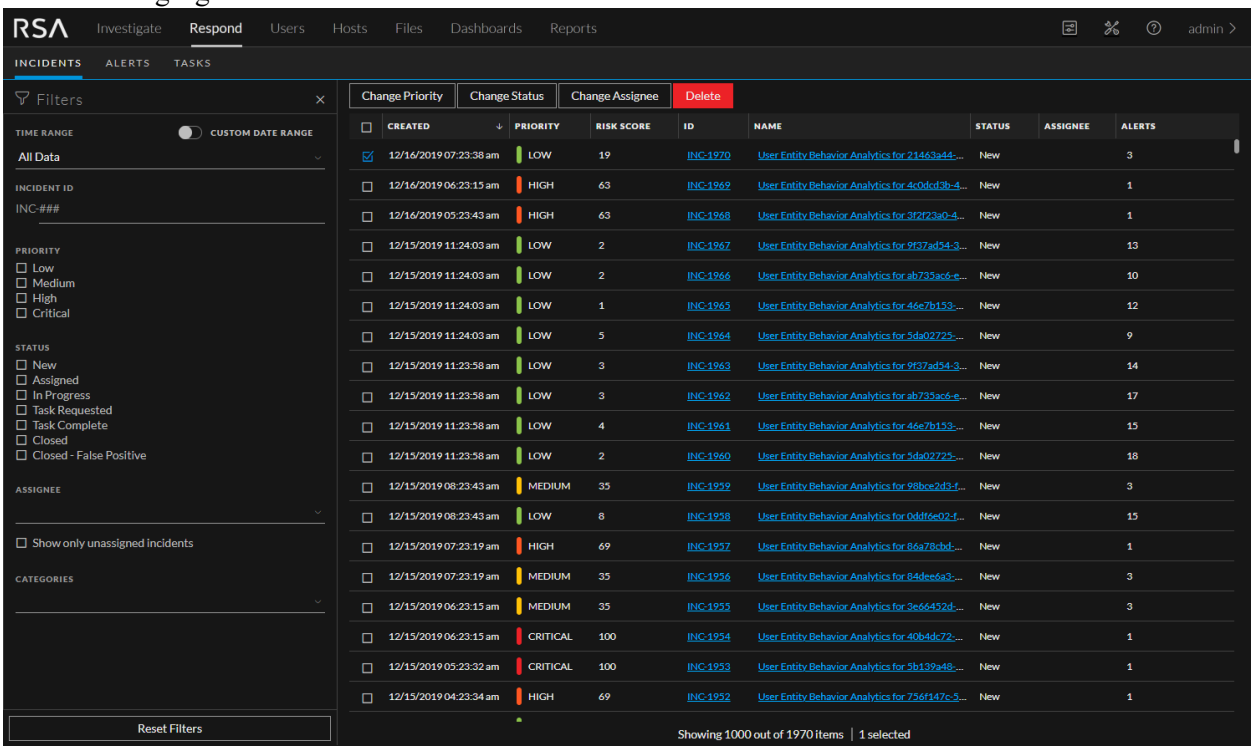
Note: This option is only available for NetWitness Platform versions 11.1 and later.

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 Platform appears to you, not other users.

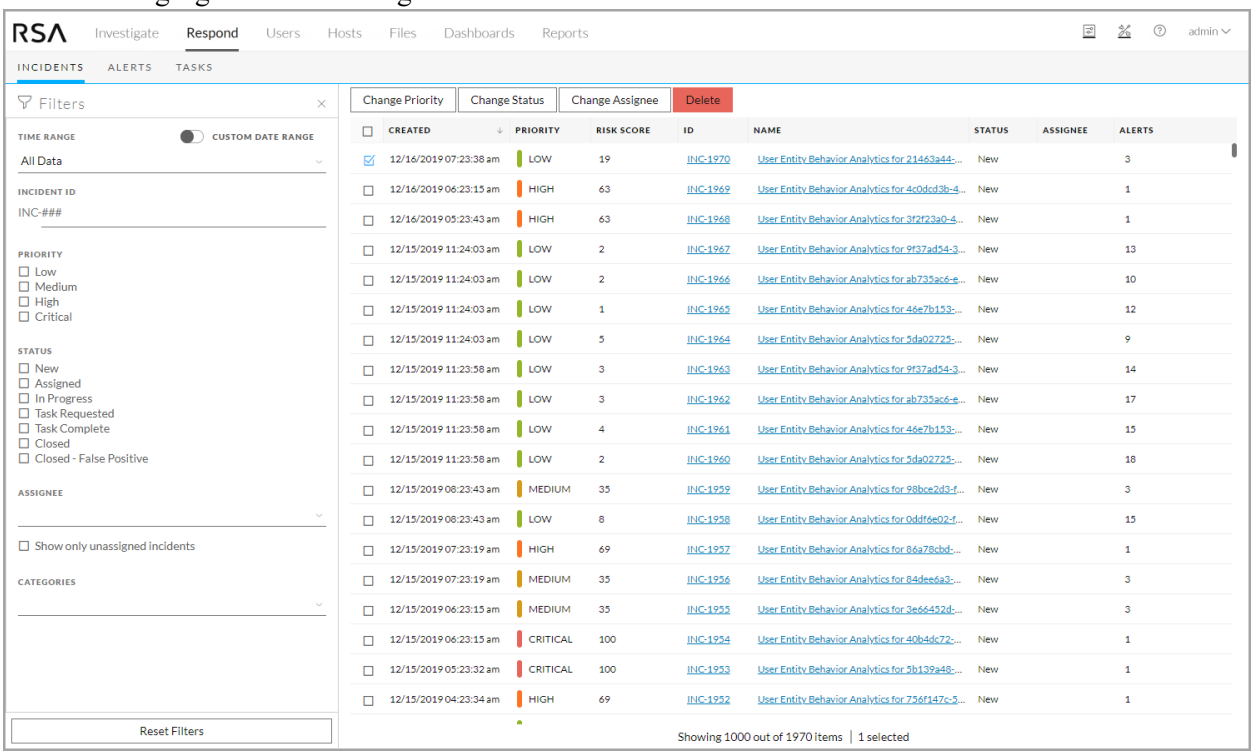
1. Open the User Preferences dialog.
2. Under **THEME**, select one of the following options:
   - **Dark**: The dark theme is best for darker environments or when you do not need as much contrast.
   - **Light**: The light theme is best for lighter environments, when you need more contrast, or when 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.



Managing Jobs

Inevitably, there are on-demand or scheduled tasks in RSA NetWitness® Platform that take a few minutes to be completed. The NetWitness Platform jobs system lets you begin a long-running task and continue using other parts of NetWitness Platform 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 Platform, 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:

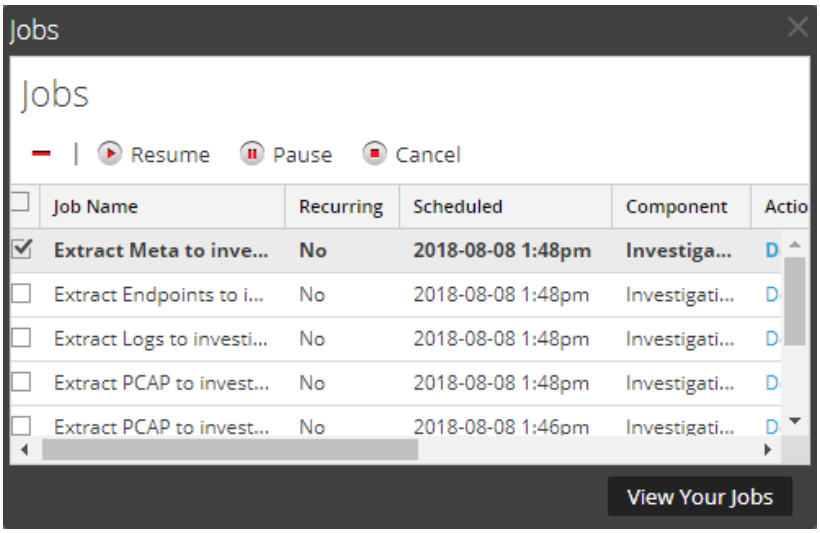
- In the user Profile Jobs panel, you see the same jobs in a full panel. These are only your jobs.
- In the System view, users with administrative privileges can view and manage all jobs for all users in a single jobs panel.

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

Display the Jobs Tray

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

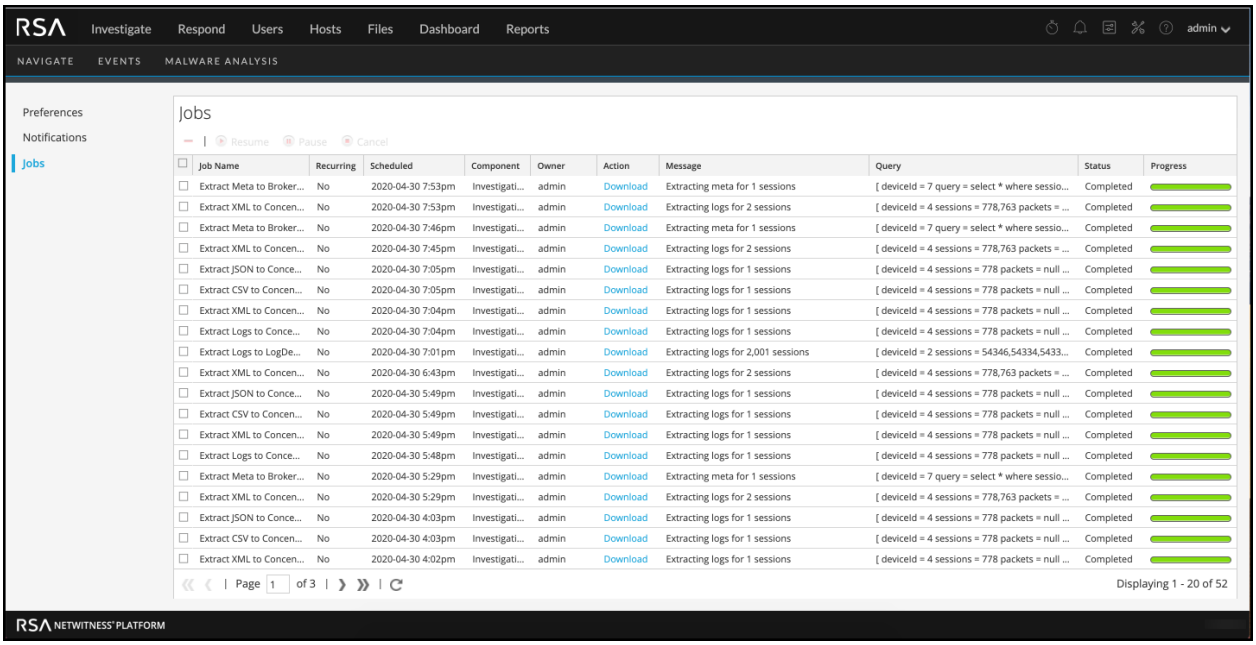
The Jobs Tray is displayed.



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 Platform 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. The Query column is available in Version 11.5 and later.



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 RSA NetWitness® Platform, 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 Platform toolbar. You can look anytime, but when a new notification is received, the Notifications icon is flagged ( ).

Examples of notifications include:

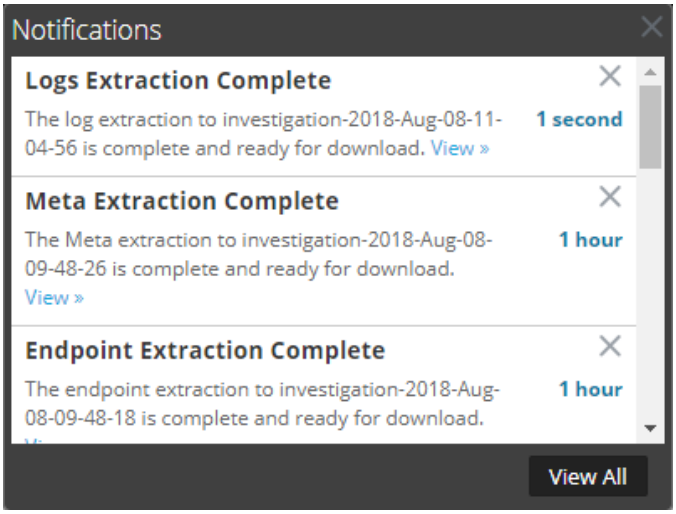
- A host upgrade completed.
- A parser push to decoders completed.
- A newer software version is available.

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.

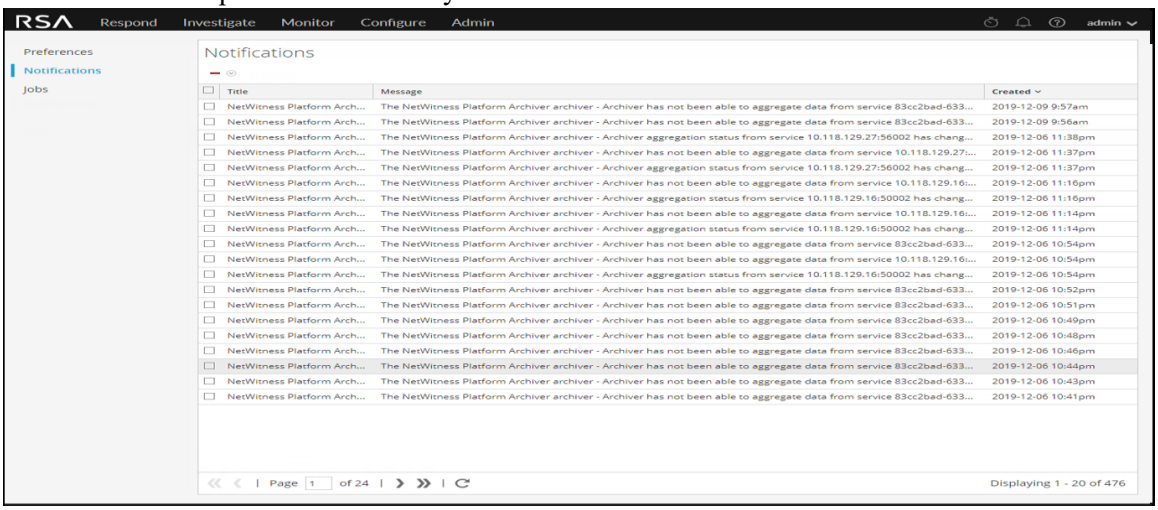


View All Your Notifications

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 Platform 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 RSA NetWitness® Platform. You can use inline help, tooltips, and online help links.

View Inline Help

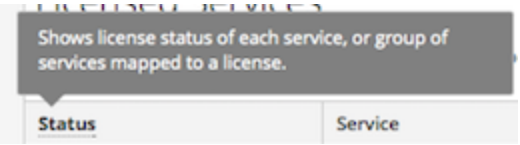
Inline help provides additional information about what to do in sections or fields that you are currently viewing in the NetWitness Platform user interface. To display inline help, hover over . The inline help shows a brief description of the element.

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:

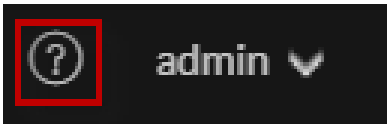


View Online Help

Online help links take you outside of NetWitness Platform to the RSA Link online documentation. This site has a complete documentation set for NetWitness Platform, 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 Platform 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 Platform toobar.



Finding Documents on RSA Link

The RSA NetWitness® Platform documentation is located on RSA Link, the RSA support portal and community. RSA Link brings all of your RSA resources together in one place. It includes advisories, product documentation, knowledge base articles, downloads, and training. To view a *Guided Tour of RSA Link*, see https://community.rsa.com/videos/21554.

Locate NetWitness Platform Documentation

NetWitness Platform Logs and Networks documentation is at the following link:
https://community.rsa.com/docs/DOC-40370

To navigate to NetWitness Platform Logs and Networks documentation:

1. On the RSA Link homepage (https://community.rsa.com), click **RSA NETWITNESS PLATFORM**.
2. On the RSA NetWitness Platform page, click **DOCUMENTATION** and select **RSA NETWITNESS PLATFORM**.

To navigate to NetWitness Endpoint 4.x documentation:

1. On the RSA Link homepage (https://community.rsa.com), click **RSA NETWITNESS PLATFORM**.
2. On the RSA NetWitness Platform page, click **DOCUMENTATION** and select **RSA NETWITNESS ENDPOINT**.

Locate RSA Content

RSA Content contains feeds, parsers, reports, and rules. It is located at the following link:
https://community.rsa.com/community/products/netwitness/rsa-content

To navigate to RSA Content:

1. On the RSA Link homepage (https://community.rsa.com), click **RSA NETWITNESS PLATFORM**.
2. On the RSA NetWitness Platform page, click **DOCUMENTATION** and select **ADDITIONAL RESOURCES** > **RSA LIVE CONTENT**.

Locate RSA Supported Event Sources

The RSA NetWitness Integrations Catalog is located at the following link:
https://community.rsa.com/community/products/netwitness/integrations/catalog

To navigate to the RSA NetWitness Integrations Catalog:

1. On the RSA Link homepage (https://community.rsa.com), click **RSA NETWITNESS PLATFORM**.
2. On the RSA NetWitness Platform page, click **DOCUMENTATION** and select **ADDITIONAL RESOURCES** > **EVENT SOURCE CONFIGURATION**.

Locate Hardware Setup Guides

The Hardware Setup Guides are at the following link:
https://community.rsa.com/community/products/netwitness/hardware-setup-guides

1. On the RSA Link homepage (https://community.rsa.com), click **RSA NETWITNESS PLATFORM**.
2. On the RSA NetWitness Platform page, click **DOCUMENTATION** and select **ADDITIONAL RESOURCES** > **HARDWARE SETUP GUIDES**.

Follow Content for Updates

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

1. Log in to RSA Link.
2. Navigate to a page or a document and in the top right corner select either **Follow** or **Actions** > **Follow**.

Send Your Feedback to RSA

Your feedback is very important to us and helps us to provide a better experience for our customers. Please send your suggestions to sahelpfeedback@rsa.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 Platform.

Problem	Troubleshooting Tip
When I log in to NetWitness Platform, 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 Platform 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 RSA Link 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 RSA Link 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 Platform application.

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

User Preferences

To adjust RSA NetWitness® Platform 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 Platform 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?

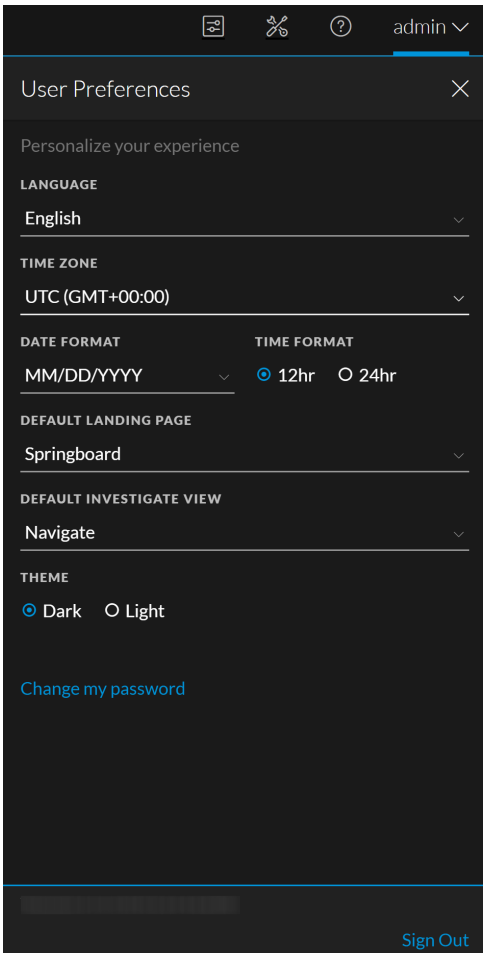
Role	I want to ...	Show me how
All	Change my Password	Change My Password Section
All	Choose my Default Landing Page	Setting Up Your Default View by SOC Role
All	Set my User Preferences	Setting User Preferences

Related Topics

- NetWitness Platform Basic Navigation

User Preferences

To access your user preferences, click your username, for example, admin.
The User Preferences dialog shows your current preferences and the NetWitness Platform version.



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

Option	Description
Language	(This option applies to NetWitness Platform 11.2 and later.) 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 Platform.
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.

Option	Description
Default Landing Page	Enables you to select the default view when you log in to NetWitness Platform. You can choose 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	(This option applies to NetWitness Platform 11.1 and later.) Select the default landing page for the Investigate view. 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 page to view the events generated for a service.
Theme	(This option applies to NetWitness Platform 11.1 and later.) 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 Platform appears to you, not other users.
Change my password	Opens the Preferences dialog where you can change your password.
Version	Shows the NetWitness Platform version.
Sign Out	Enables you to log out of NetWitness Platform.

Any selections that you make become effective immediately.

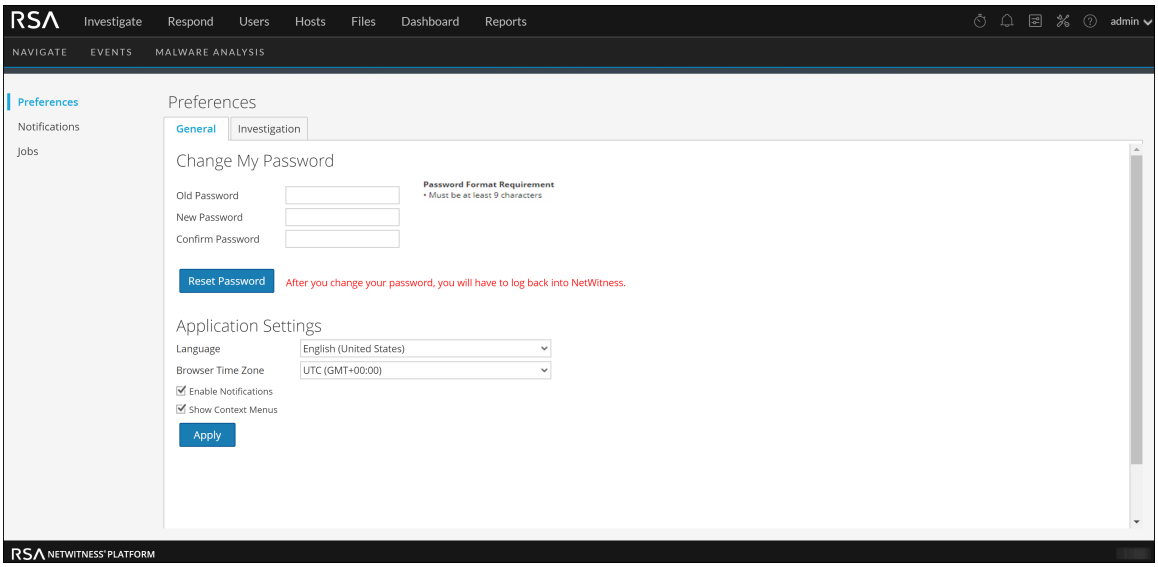
Preferences

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 Springboard, Investigate view [Events (formerly Event Analysis)], Respond, Users, Hosts, Files, and some Configure views, select your username, for example

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

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

Application Settings Section

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

Option	Description
Language	(This option applies to NetWitness Platform 11.2 and later.) 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 Platform. Your time zone preference is displayed on the toolbar.
Enable Notifications	This checkbox enables and disables notifications for your user account. By default, NetWitness Platform 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

RSA NetWitness® Platform 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 Platform, 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 Platform 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.

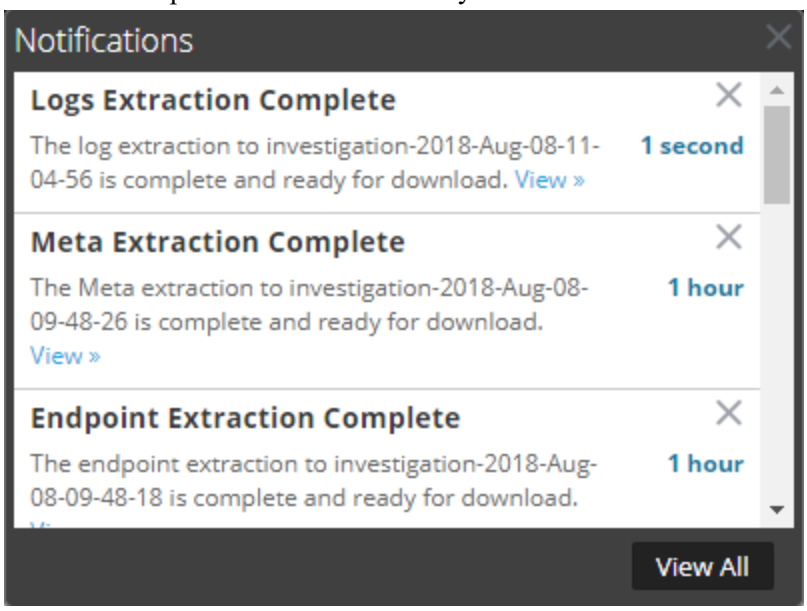
What do you want to do?

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

Quick Look

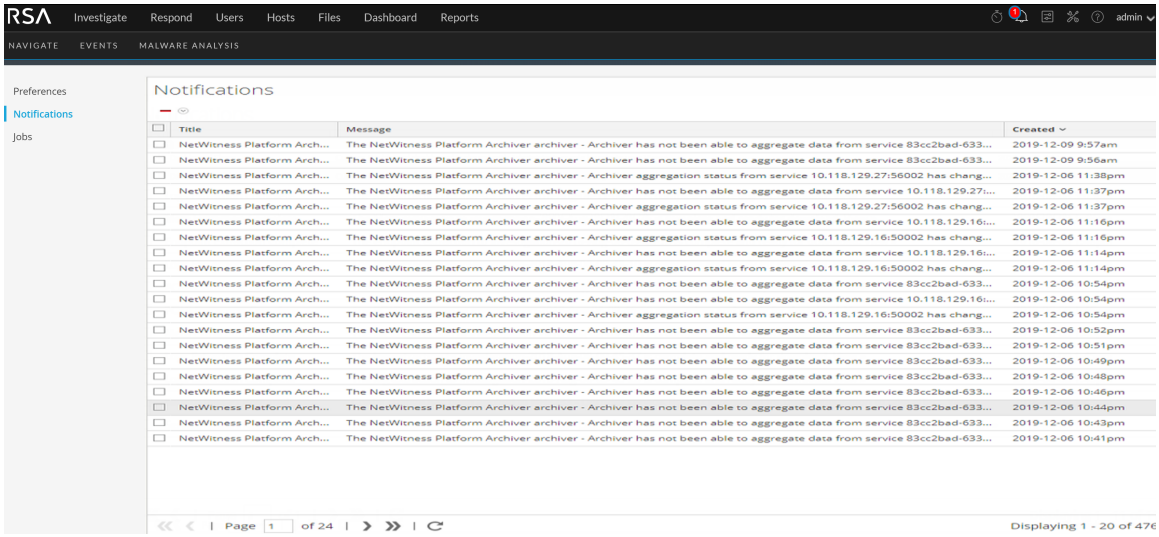
To access the Notifications panel, do one of the following:

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



- In the upper right corner of the NetWitness Platform 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 RSA NetWitness® Platform 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 Platform 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 Platform, you can open a quick view of your jobs from the NetWitness Platform 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?

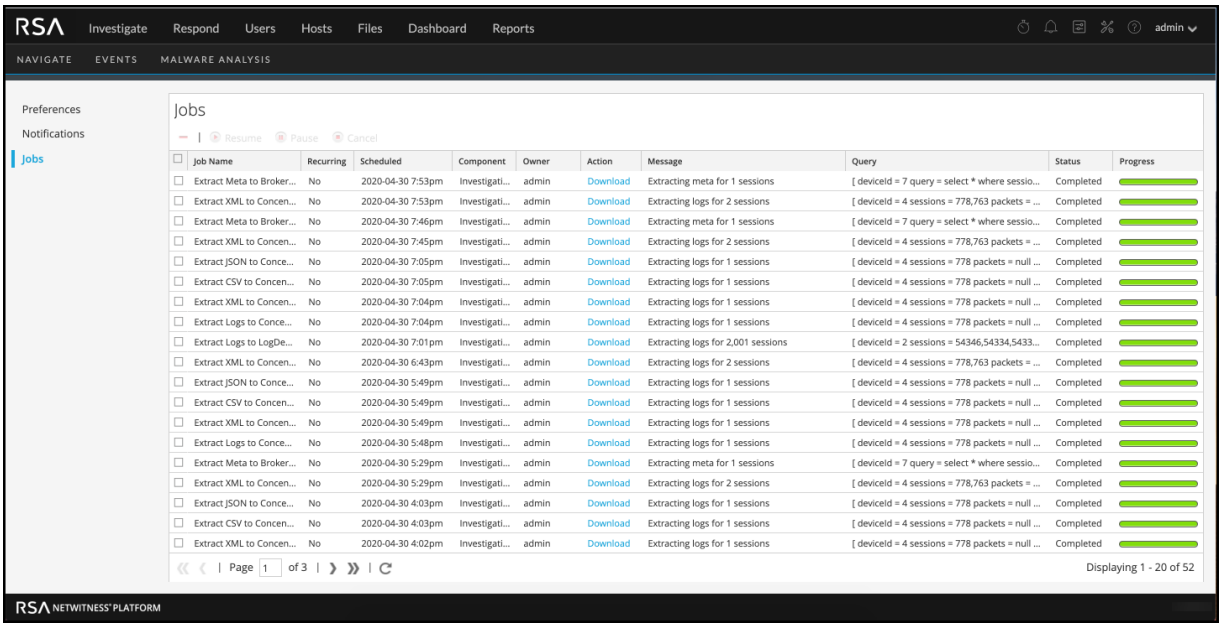
Role	I want to ...	Show me how
All	Pause and Resume a Scheduled Job	Managing Jobs
All	Cancel or Delete a Job	Managing Jobs
All	Download a Job	Managing Jobs

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

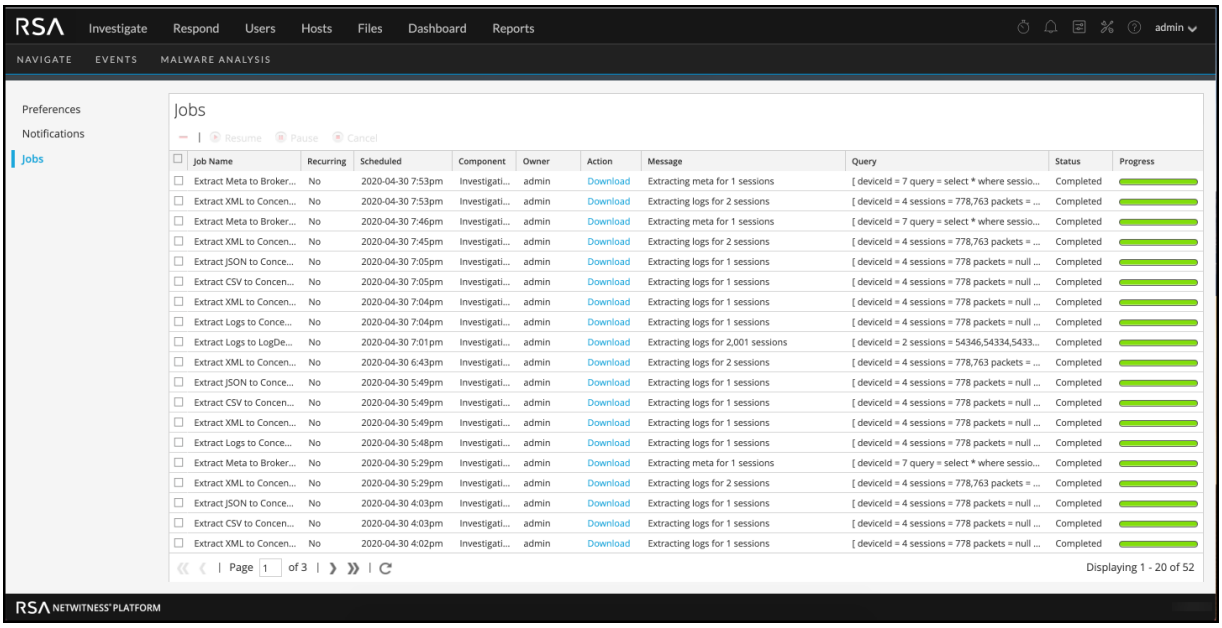
Quick Look

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

- In the upper right corner of the NetWitness Platform 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.

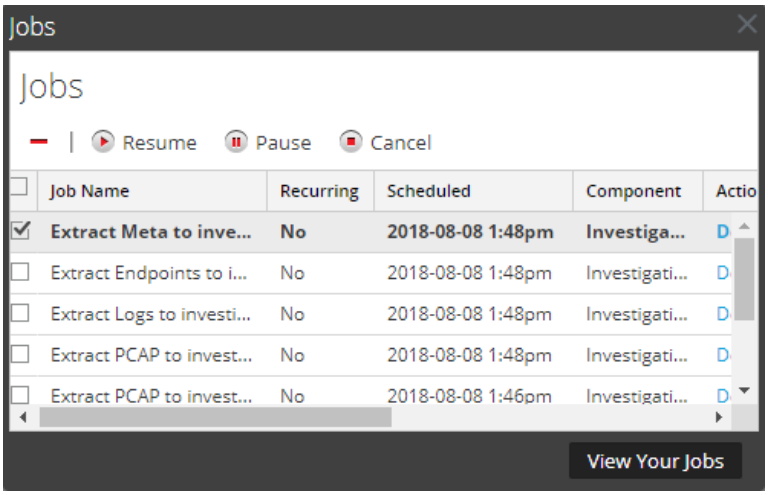


- Go to **(Admin) > System**, and in the options panel, select **Jobs**.
  The Jobs panel in the Admin System view is displayed. It shows the jobs for all users.



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 Platform 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 Platform 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**.