RSA NETWITNESS® SUITE

# Getting Started Guide

for Version 11.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

## Contact Information

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

## Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

## License Agreement

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

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

## Third-Party Licenses

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

## Note on Encryption Technologies

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

## Distribution

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

September 2018

# Contents

# Getting Started with NetWitness Suite

## Overview

RSA NetWitness Suite is a powerful threat detection suite that enables Security Operation Centers (SOCs) to quickly locate, prioritize, and triage threats. NetWitness Suite 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 Suite is more powerful than ever, but it is easier for Tier 1 Analysts to use because it automates the process of identifying and prioritizing suspicious threats. In addition, Tier 2 and Tier 3 analysts can hunt for and locate threats using new analysis tools.

## Architecture

RSA NetWitness Suite is a distributed and modular system that enables highly flexible deployment architectures that scale with the needs of the organization. NetWitness Suite allows administrators to collect three types of data from the network infrastructure, packet data, log data, and endpoint data. If NetWitness Endpoint 4.4, 4.4.0.0, or later is installed and configured, endpoint event data is also collected. 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 reconstructs 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/Concentrator pairs throughout the infrastructure.
- **Real-time Alerting**. The NetWitness Suite **Event Stream Analysis (ESA)** service provides advanced stream analytics such as correlation and complex event processing at high throughputs and low latency. It is capable of processing 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 modules for detecting Command and Control traffic.

- **NetWitness Server**. The NetWitness Server provides Reporting, Investigation, Administration, and other aspects of the user interface.
- **Capacity**. NetWitness Suite 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 longer-term analytic and data-retention needs.

The NetWitness Suite 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 Suite system has been optimized to run on virtualized infrastructure.

The System Architecture comprises these major components: Decoders, Brokers, Concentrators, Archivers, ESA, and Warehouse Connectors. NetWitness Suite 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 Hybrid or Endpoint Log Hybrid. The Response-Server service is also required and is used to prioritize alerts.

The following table provides a synopsis of each major component.

| System Component | Description |
|---|---|
| **Decoder / Log Decoder** | • NetWitness Suite collects packet, log, and endpoint data.<br>• 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.<br>• A Log Decoder can collect four different log types - Syslog, ODBC, Windows eventing, and flat files.<br>• Windows eventing refers to the Windows 2008 collection methodology and flat files can be obtained via SFTP.<br>• Both types of Decoders ingest raw transactional data that is enriched, closed out, and aggregated to other NetWitness Suite components.<br>• The process for ingesting and parsing transactional data is a dynamic and open framework. |
| **Endpoint Hybrid or Endpoint Log Hybrid** | • Collects and manages endpoint data from hosts.<br>• Generates metadata for investigation, analysis, alerting, and reporting.<br>• Collects logs from Windows hosts, and all other event sources that are supported for the Log collection in the NetWitness Suite. |
| **Concentrator** | • Provides index and query capability to NetWitness Collections.<br>• Can optionally forward data to ESA. |
| **Broker** | • Distributes NetWitness Collection access across many Concentrators or Archivers, making the entire NetWitness Suite enterprise appear as a single collection. |

| System Component | Description |
|---|---|
| **Archiver** | • The Archiver service enables long-term log archiving by indexing and compressing log data and sending it to archiving storage.<br>• The archiving storage is optimized for long-term data retention, and compliance reporting.<br>• Archiver stores raw logs and log metadata from Log Decoders for long term-retention, and it uses Direct-Attached Capacity (DAC) for storage.<br>**Note:** Raw packets and packet metadata are not stored in the Archiver. |
| **Event Stream Analysis (ESA)** | • The Event Stream Analysis service provides event stream analytics such as correlation and complex event processing at high throughputs and low latency. It is capable of processing large volumes of disparate event data from Concentrators.<br>• ESA uses advanced Event Processing Language that allows users to express filtering, aggregation, joins, pattern recognition, and correlation across multiple disparate event streams.<br>• ESA helps to perform powerful incident detection and alerting.<br>• The RSA Automated Threat Detection functionality includes preconfigured ESA analytics modules for detecting Command and Control traffic. |

## Core Versus Downstream Components

In NetWitness Suite, 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 Suite

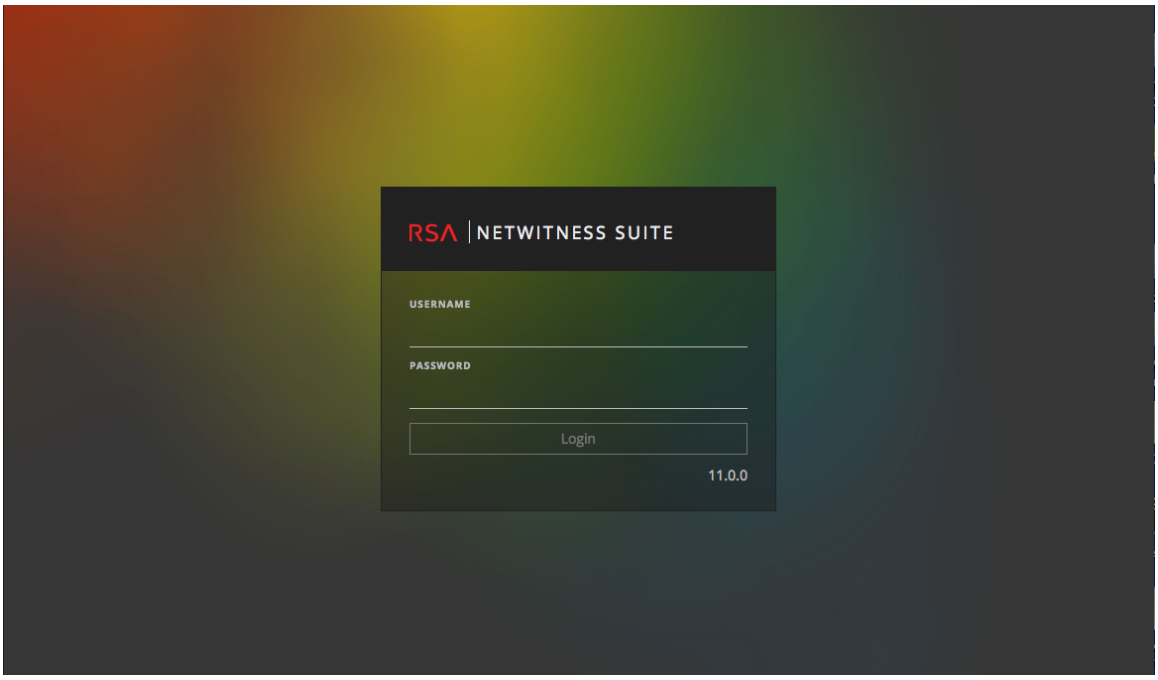
Logging in to NetWitness Suite can vary based on your environment. You may have an internal user account or an external user account. Internal user accounts are local to the NetWitness Suite and internal users can log in to NetWitness Suite and receive role-based permissions. External user accounts authenticate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

1. Use an 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 IP address of your NetWitness server.

   The login screen is displayed.




2. Type your username and password, and then click **Login**.

   If your login is successful, you will be logged in to the landing page specified in your user preferences.

**Note:** NetWitness Suite supports modern (or current) versions of the latest browsers.

### If you are locked out:

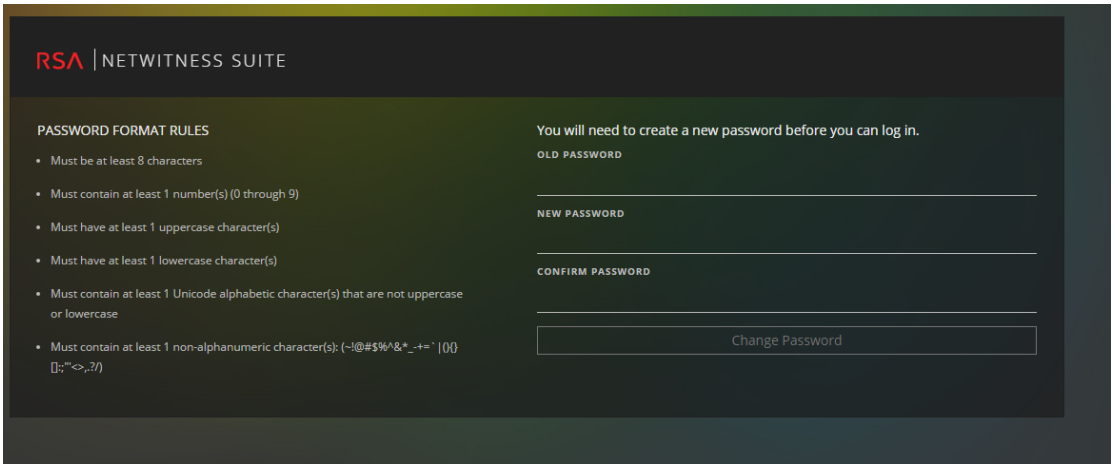
**Note:** This information applies to internal accounts only. It does not apply to Active Directory or PAM accounts.

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

### If you have a new account or your account is expired:

**Note:** This information 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 Suite:

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 Suite

### To log off from the Respond and some Investigate views:

1. In the main menu bar, select  .
2. In the User Preferences, click **Sign Out**.

### To log off from the other views:

In the main menu bar, select  > **Sign Out**.

# Changing Your Password

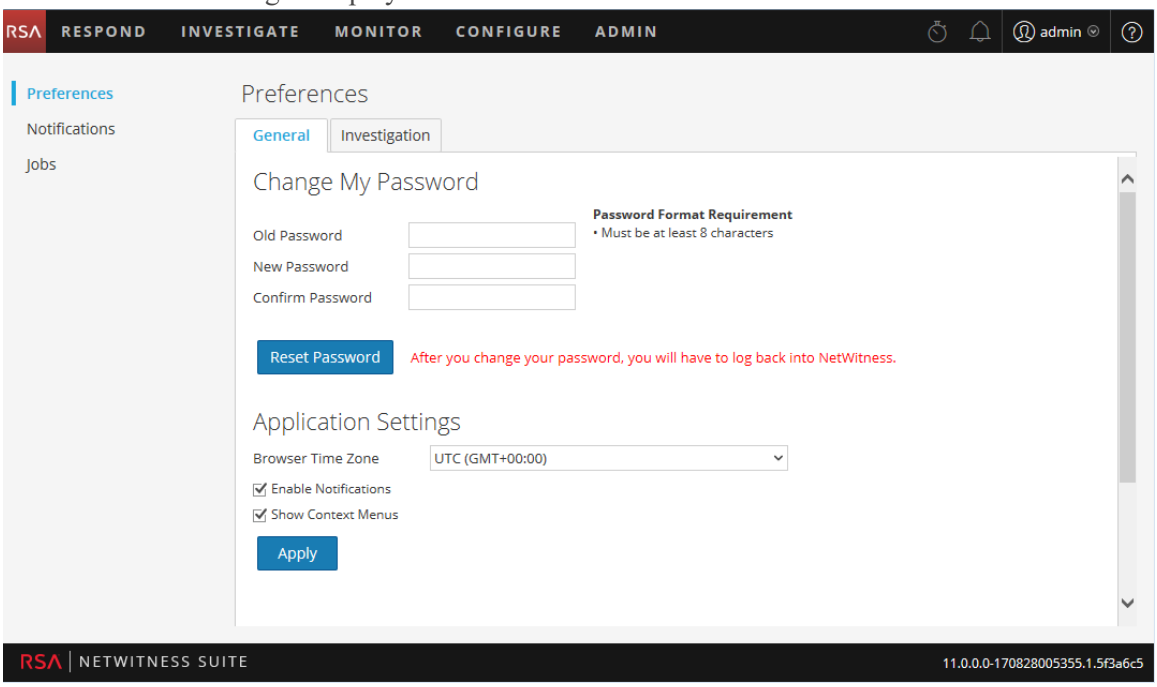
You can change the password that you use for NetWitness Suite authentication at any time in your user preferences. Your Administrator defines the appropriate password strength requirements for your NetWitness Suite password, such as minimum password length and minimum number of uppercase, lowercase,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

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

### To change your password:

1. Do one of the following:
   - For most views, such as Investigate, Monitor, Configure, or Admin, select  > **Profile**.
   - In the Respond and some Investigate views (Event Analysis, Hosts, and Files), select  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 Suite 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 Suite for the changes to take effect. The new password becomes effective the next time you log in to NetWitness Suite.

# Identify Your Role

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

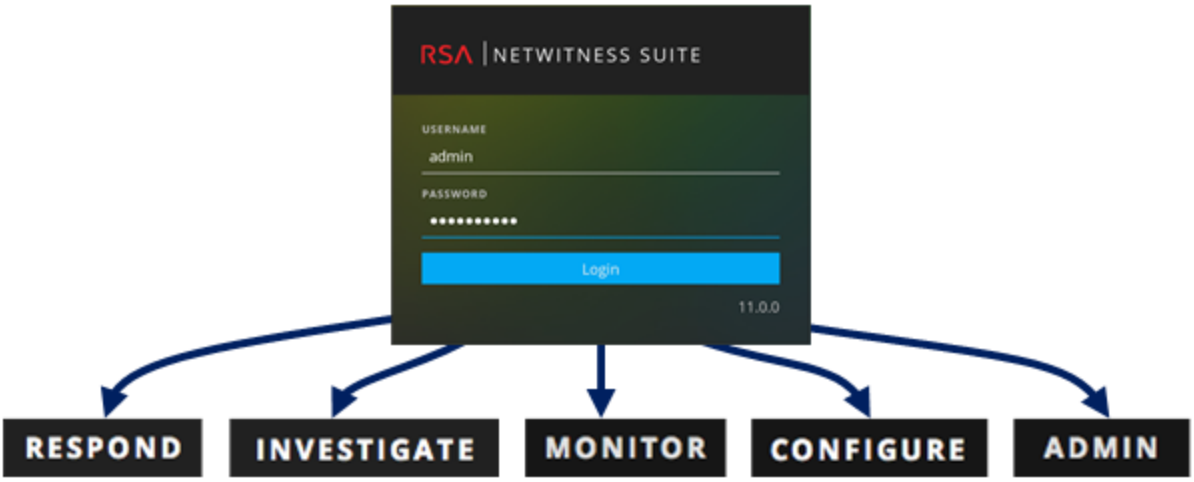
- Investigate new threat intelligence
- Evaluate and create new feeds
- Create correlation rules to flag indicators of compromise

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 Suite Basic Navigation

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




- **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 Suite here.
  For legacy 10.6 users, this view was known as the Incident Management view. The Alerts List in the Respond view replaces the ESA 10.6 Alerts > Summary view.
- **INVESTIGATE**: This view is primarily for advanced Threat Hunters, who prefer to manually hunt for threats using NetWitness Suite 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.
- **MONITOR**: This view is for all users. You can view dashboards and reports on different areas of interest depending on your user permissions. NetWitness Suite opens to this view by default.
  For legacy 10.6 users, this is the Dashboard view.
- **CONFIGURE**: This view is for Threat Intel (content) personnel, who configure data sources and inputs to NetWitness Suite. Threat Intel personnel use this area to download and manage Live content. They can also create and manage incident and ESA rules.
  For legacy 10.6 users, this view contains Live, Incidents > Configure, and Alerts > Configure from the previous version.

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

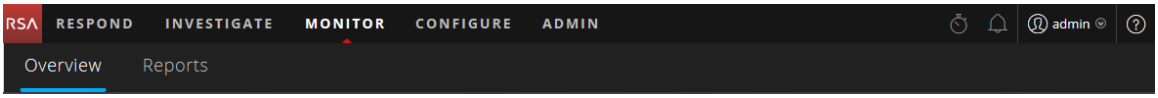
  For legacy 10.6 users, this is the Administration view less the sections added to the Configure view.

## 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 browser window at any time.

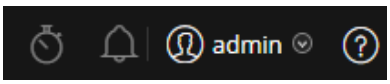

## Secondary Menus

Some 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 MONITOR menu.

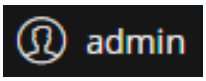
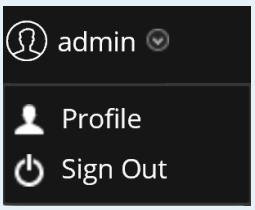



## Additional Options

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




The following table describes these common options:

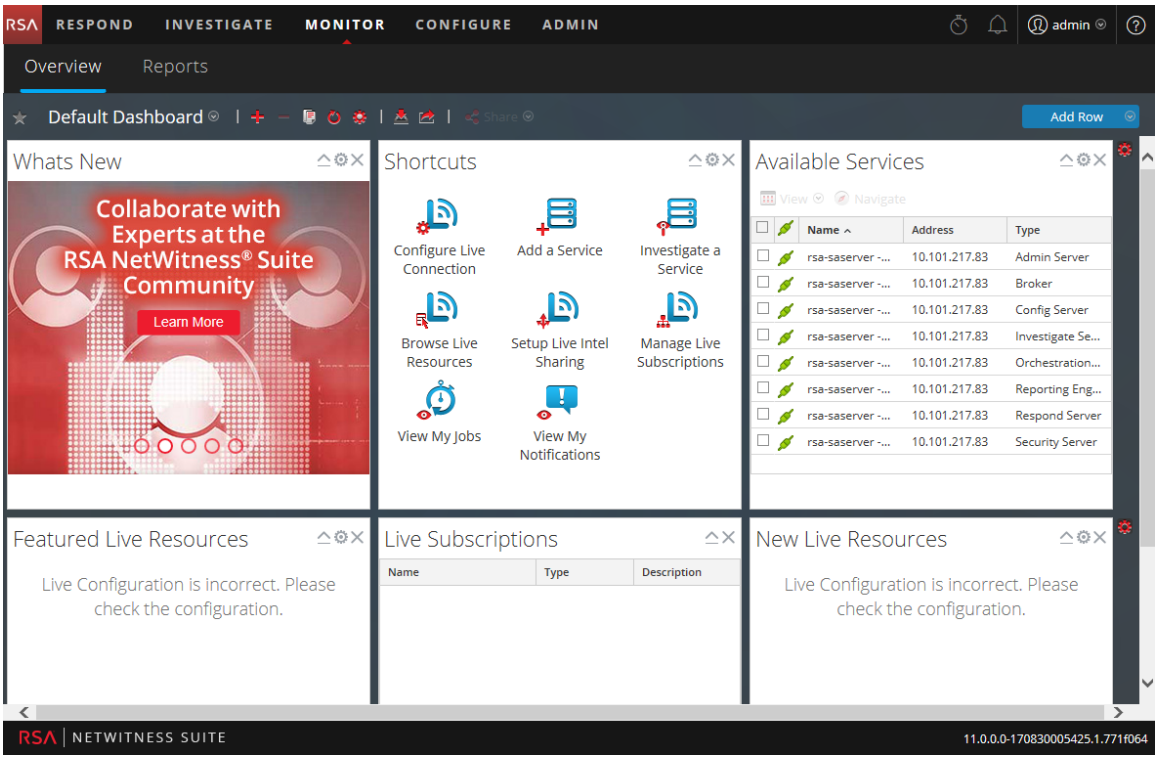
| Common Option | Name | Description |
|---|---|---|
|  | Jobs | In the INVESTIGATE, MONITOR, CONFIGURE, and ADMIN views, click this icon to view and manage your jobs in the Jobs tray. Jobs are on-demand or scheduled tasks that take some time to complete in the NetWitness Suite application. |
|  | Notifications | 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 Suite. |
|  | 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 Suite. |
|  | Help | Click this icon to view NetWitness Suite help topics. |

## Main Views

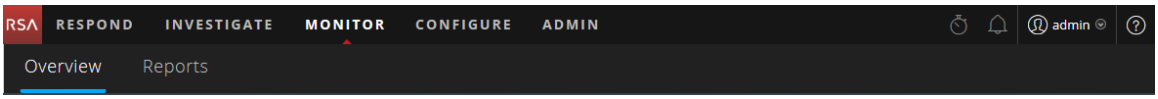
The following sections explain the main views.

# MONITOR

The MONITOR view contains the NetWitness Suite dashboard. Monitor offers preconfigured dashboards and reports that you can use or you can create your own.




## MONITOR Menu




The MONITOR menu has the following options:

- **Overview**: The Overview view enables you to view and manage your dashboards. 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

For legacy 10.6 users, this was the Dashboard view.

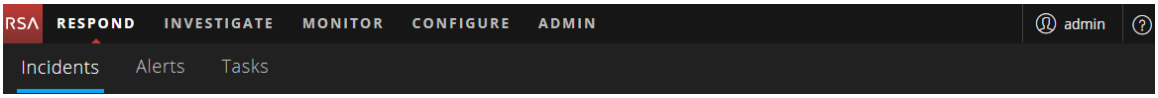
- **Reports**: The Reports view enables you to view and manage reports relevant to your SOC role according to your assigned permissions.

| What can I do here? | Path | Show me how |
|---|---|---|
| Select a Dashboard | MONITOR > Overview | See Managing Dashboards. |
| Create a Dashboard | MONITOR > Overview | See Managing Dashboards. |
| Manage Dashboards | MONITOR > Overview | See Managing Dashboards. |
| View a Report | MONITOR > Reports > View | See the *Reporting Guide*. |
| Manage Reports | MONITOR > Reports > Manage | See the *Reporting Guide*. |

## 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

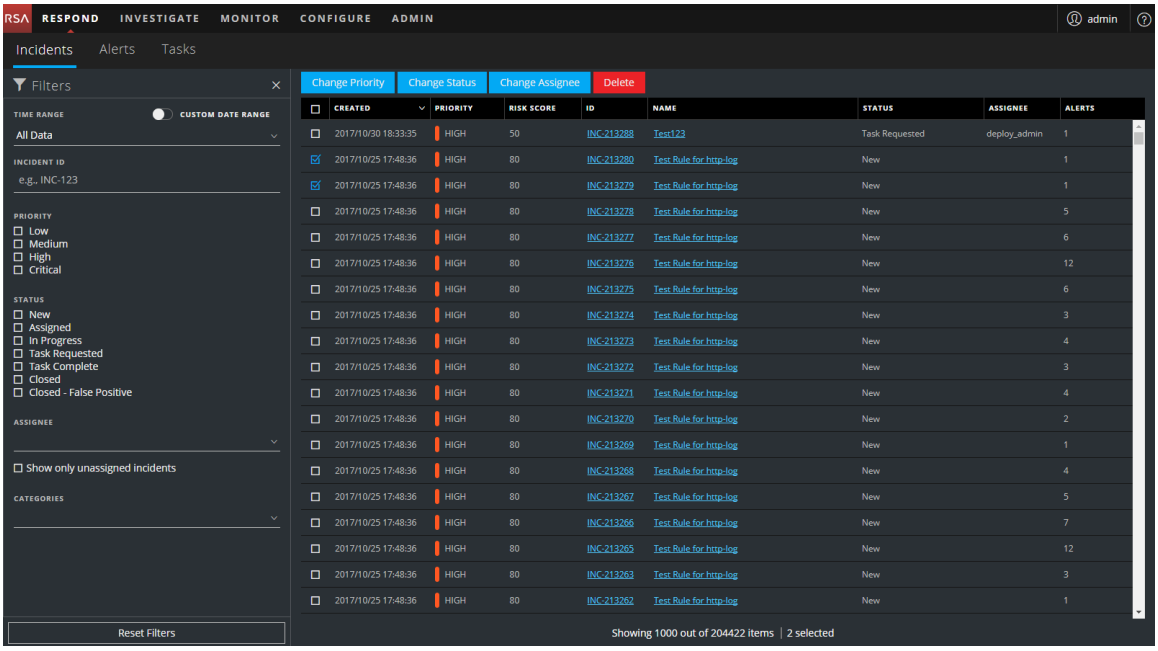



The RESPOND menu has the following options:

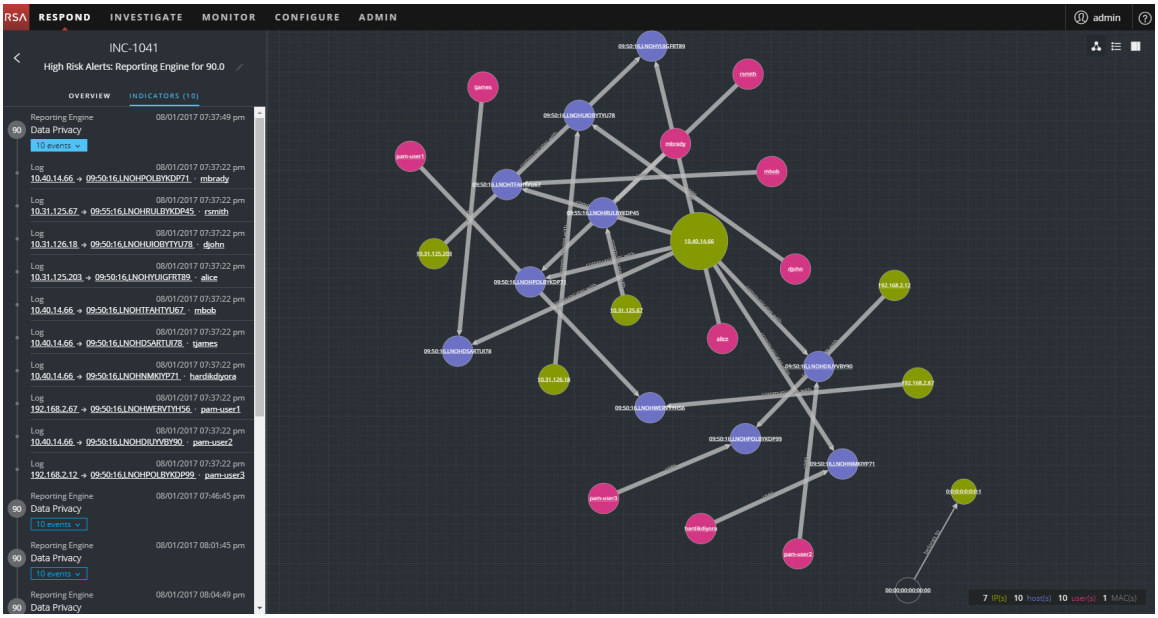
- **Incidents**: The Incidents List view contains a list of all incidents with basic information. The Incident Details view provides extensive details about the incident.

- **Alerts**: The Alerts List and Alert Details views provide information about all of the threat alerts and indicators received byNetWitness Suite 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 - Incident List view.

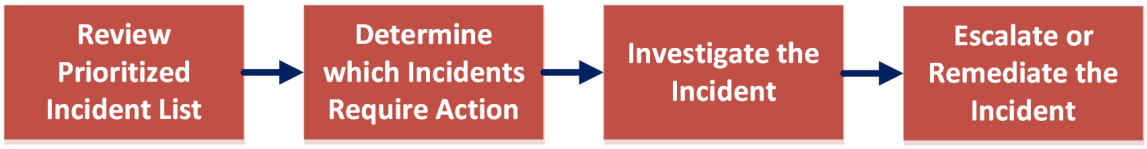



The following figure shows an example of the Respond view - Incident Details view.




When using NetWitness Suite as your case management tool, you can also case manage incidents from this view. New incidents appear at the top of the incident queue in priority order and incidents in progress are below the new incidents.

The following figure shows a high-level Respond view workflow.



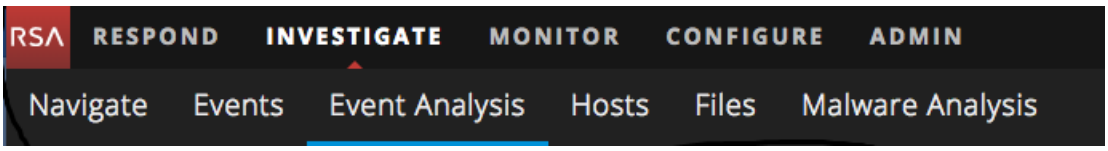

In the Respond view, analysts look at the prioritized list of incidents and determine which incidents require action. They click an incident for a clear picture of the incident with supporting details and they can investigate the incident further. Analysts can then determine how to respond to the threat,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

| What can I do here? | Path | Show me how |
|---|---|---|
| View prioritized incident lists | RESPOND > Incidents (Incident 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*. |

# INVESTIGATE

The Investigate view presents six different views into a set of data, allowing analysts to see metadata, endpoint data, logs, events, and potential indicators of compromise. In addition to investigating data on a specific service, you can pivot into Investigate from Respond, the Monitor 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 of the six Investigate views, then continue the investigation 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 *NetWitness Investigate User Guide* provides detailed information.

## INVESTIGATE Menu



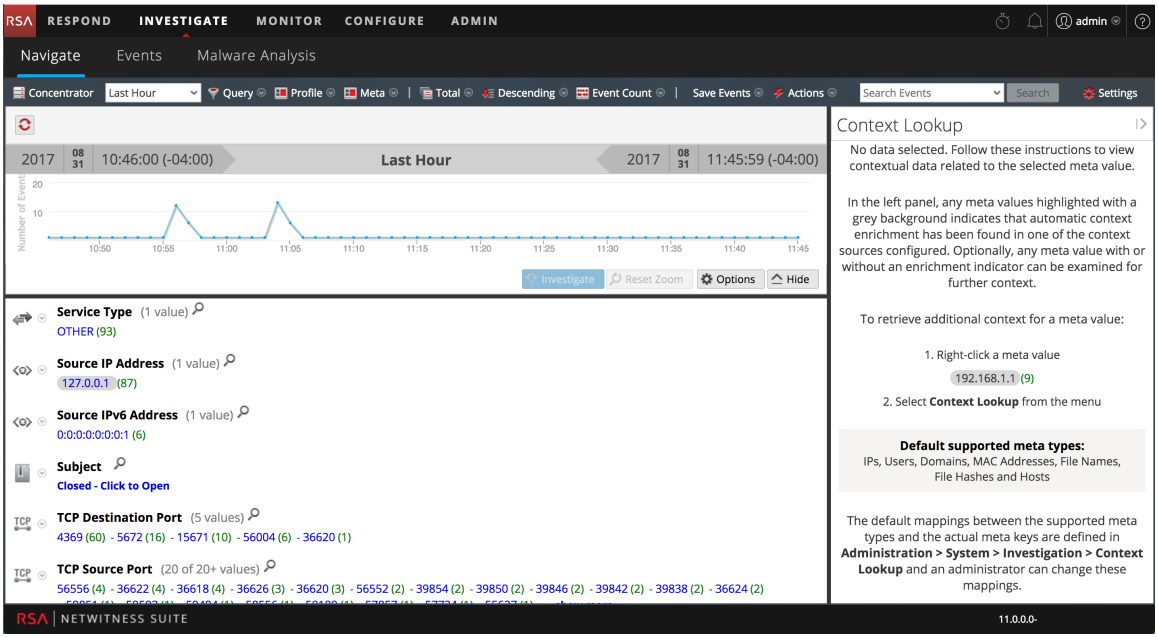

The INVESTIGATE menu has the following options:

- **Navigate**: The Navigate view provides a list of meta keys and meta values with a focus on metadata. You can drill into the data, open a selected event in the Events view or the Event Analysis view, view a reconstruction of an event, search for events, look up additional context from the Context Hub service, and configure Navigate view preferences.
- **Events**: The 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, open a selected event in the Event Analysis view, view a reconstruction of the event, conduct event analysis, and configure Events view preferences.
- **Event Analysis**: The Event Analysis view provides a list of events with focus on metadata and raw data. You can view a reconstruction that offers helpful cues to identify points of interest in a reconstruction, jump to the Hosts view, pivot to standalone Endpoint, look up data in Live, and do external lookups.
- **Hosts view**: (Version 11.1 and later) The Hosts view lists all hosts with a NetWitness Endpoint Insights Agent running. For every host, you can view processes, drivers, DLLs, files (executables), services, and autoruns that are running, and information related to logged-in users. From the Hosts view, you can go to the Navigate and Event Analysis views.
- **Files view**: (Version 11.1 and later) The Files view lists all unique files found in your deployment and their associated properties. For each file, you can view details such as file

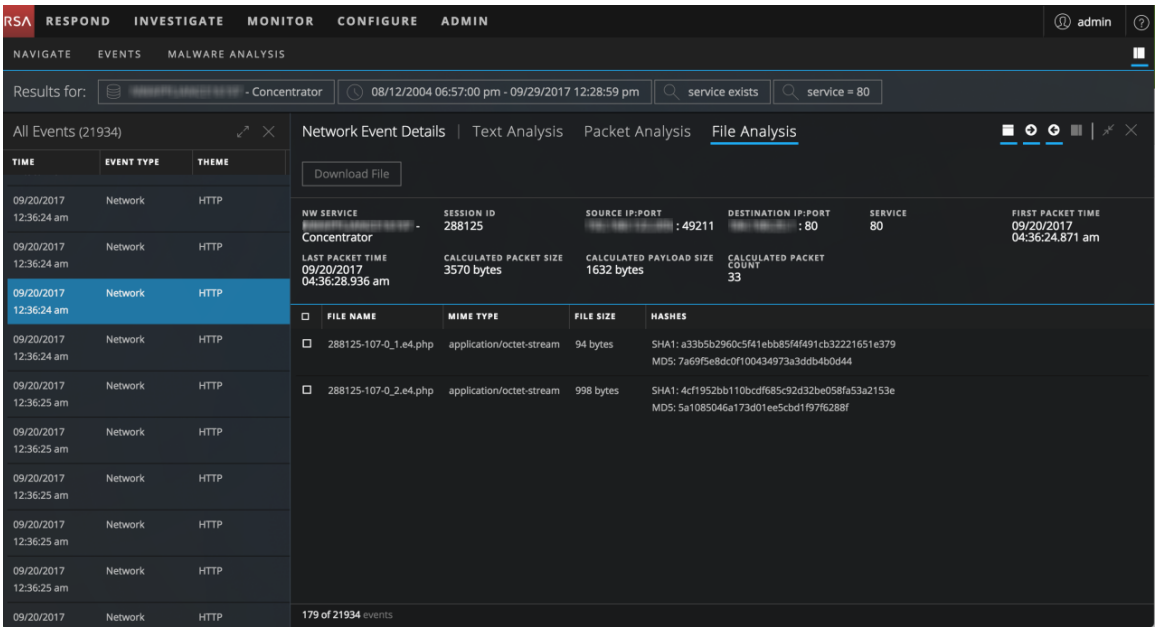
size, entropy, format, company name, signature, and checksum. From the Files view, you can go to the Navigate and Event Analysis views.

- **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.

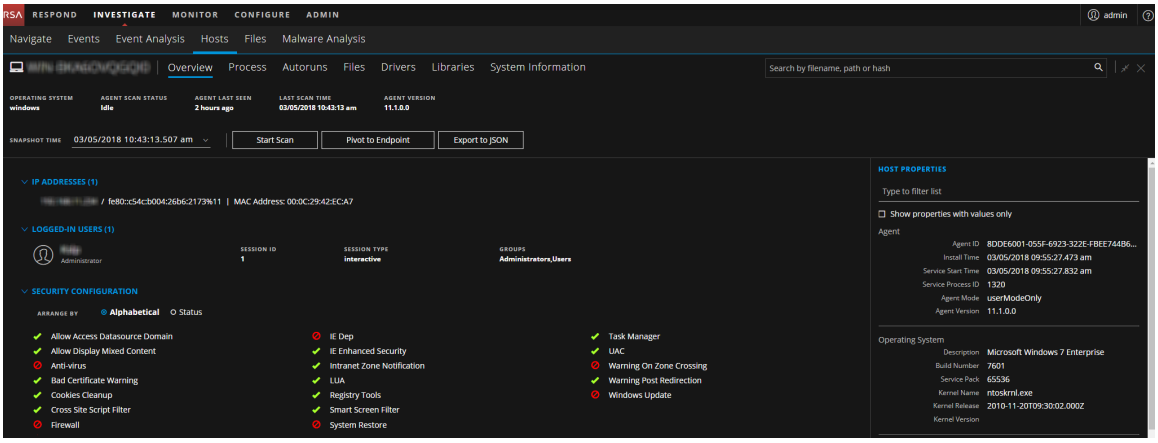
The following figure shows the Investigate view - Navigate view.



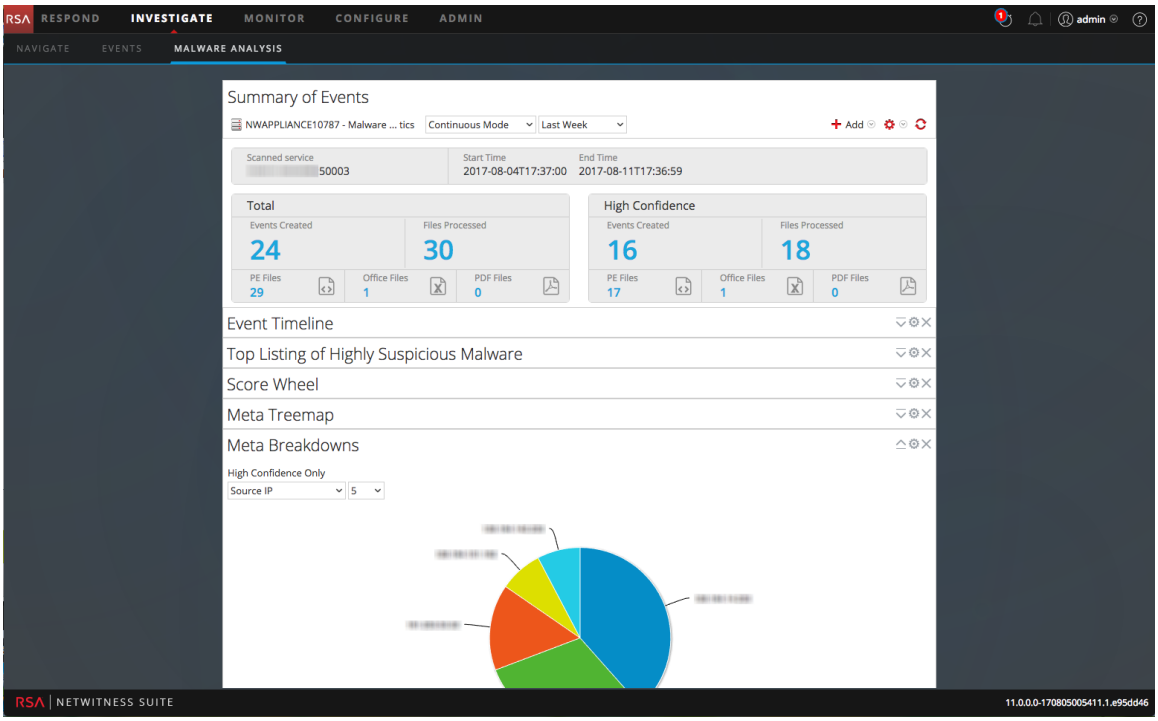

The following figure shows the Investigate view - Event Analysis view.



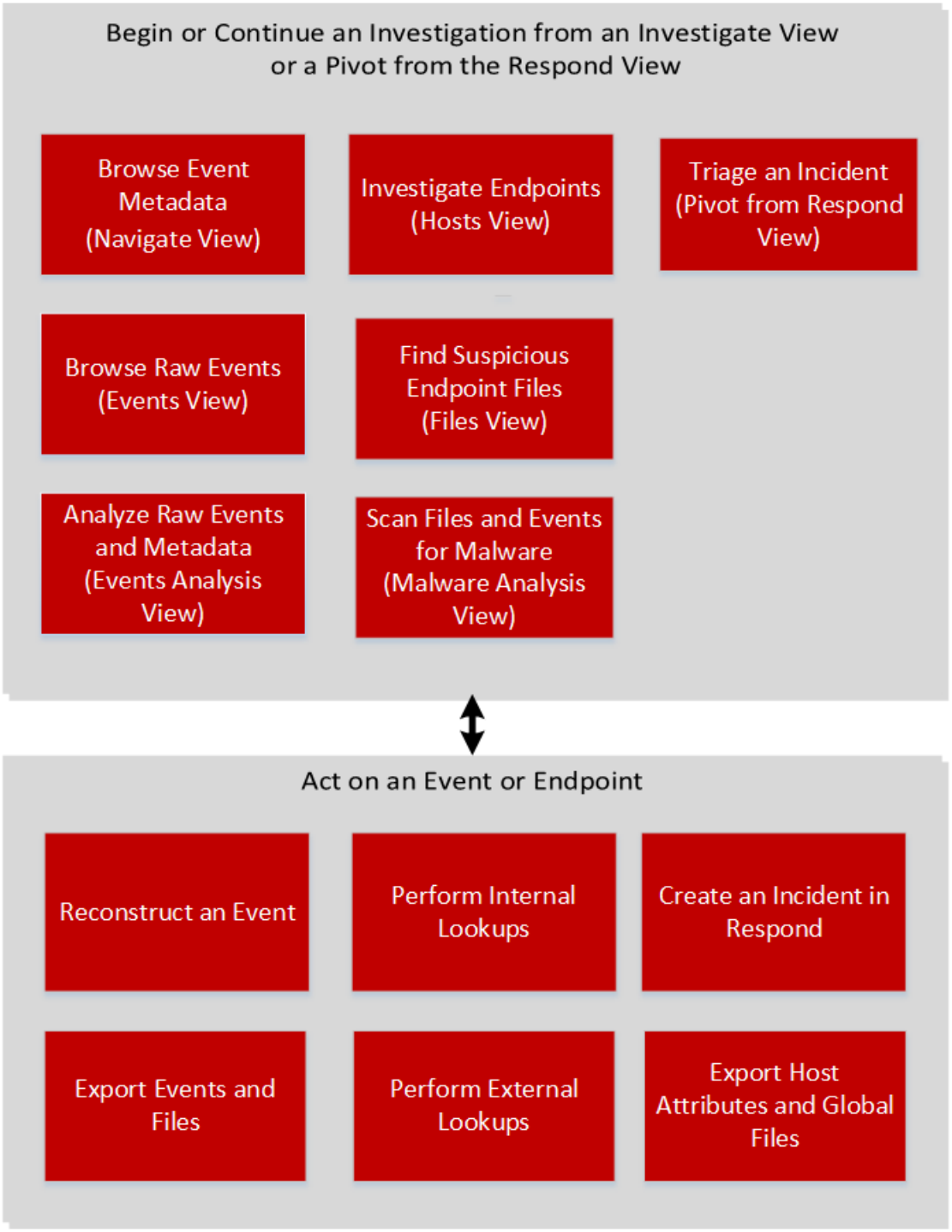

The following figure shows the Hosts view - Host Details view.




The following figure shows the Malware Analysis Summary of Events.




The following figure shows a high-level workflow of the Investigate view.

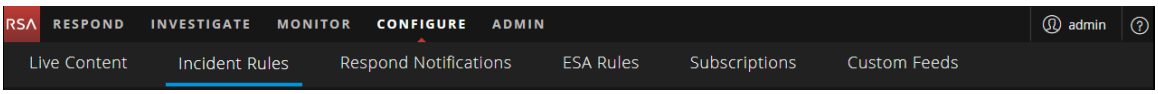

Begin or Continue an Investigation from an Investigate View or a Pivot from the Respond View
Browse Event Metadata (Navigate View)
Investigate Endpoints (Hosts View)
Triage an Incident (Pivot from Respond View)
Browse Raw Events (Events View)
Find Suspicious Endpoint Files (Files View)
Analyze Raw Events and Metadata (Events Analysis View)
Scan Files and Events for Malware (Malware Analysis View)
Act on an Event or Endpoint
Reconstruct an Event
Perform Internal Lookups
Create an Incident in Respond
Export Events and Files
Perform External Lookups
Export Host Attributes and Global Files

| What can I do here? | Path | Show me how |
|---|---|---|
| Browse Event Metadata | Navigate view | See "Investigating Metadata in the Navigate View" in the *NetWitness Investigate User Guide*. |
| Browse Raw Events | Events view | See "Examining Raw Events in the Events View" in the *NetWitness Investigate User Guide*. |
| Analyze Raw Events and Metadata | Event Analysis view | See "Examining Metadata and Raw Events in the Event Analysis View" in the *NetWitness Investigate User Guide*. |
| Investigate Endpoints | Hosts view | See "Investigating Hosts and Files" in the *NetWitness Investigate User Guide*. |
| Find Suspicious Endpoint Files | Files view | See "Investigating Hosts and Files" in the *NetWitness Investigate User Guide* |
| Scan Files and Events for Malware | Malware Analysis view | See "Conducting Malware Analysis" in the *NetWitness Investigate User Guide* |

## CONFIGURE

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

NetWitness Suite services and software. When you subscribe to a resource, you agree to receive updates on a regular basis from RSA Live Services.
For Legacy 10.6 users, this was Live > Search.

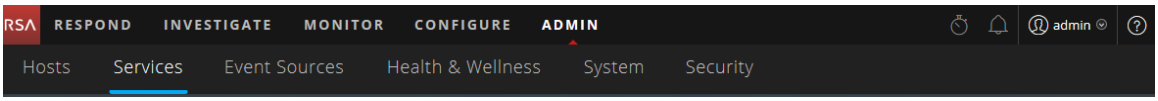
- **Incident Rules**: The Incident Rules view enables you to create incident rules with various criteria to automatically create incidents. You can view prioritized incidents in the Respond view.
  For Legacy 10.6 users, this was Incidents > Configure. In 11.1 and later, Aggregation Rules are known as Incident Rules.
- **Respond Notifications**: The Respond 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 problem 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.
  For Legacy 10.6 users, this was Alerts > Configure.
- **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 Suite, you configure the connection and synchronization between the CMS server and NetWitness Suite.
  For Legacy 10.6 users, this was Live > Configure.
- **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 Suite uses feeds to create metadata based on externally defined metadata values. A feed is a list of data that is compared to sessions as they are captured or processed. For each match, additional metadata is created.
  You can create custom feeds to provide extra metadata extraction, for example, to accommodate custom network applications.
  For Legacy 10.6 users, this was Live > Feeds.

| 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*. |
| Create incidents automatically. | CONFIGURE > Incident Rules | See the *NetWitness Respond Configuration Guide*. |
| Configure Respond notifications. | CONFIGURE > Respond Notifications | See the *NetWitness Respond Configuration Guide*. |
| Configure alerts. | CONFIGURE > ESA Rules | See the *Alerting with ESA Correlation Rules User Guide*. |
| Set up Live Services Services on NetWitness Suite | CONFIGURE > Subscription | See the *Live Services Management Guide*. |
| Set up and maintain custom and identity feeds. | CONFIGURE > Custom Feeds | See the *Live Services Management Guide*. |

## ADMIN

In the Admin view, Administrators can manage network hosts and services; monitor the health and Wellness of NetWitness Suite; 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.
- **Health & Wellness**: The Health & Wellness view enables you to monitor the health of the NetWitness Suite hosts and services in your network environment.
- **System**: The System view enables you to set global NetWitness Suite 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 Suite versions and configure the local licensing server.
- **Security**: The Administration Security view provides the capability to manage user accounts, manage user roles, map external groups to NetWitness Suite roles, and modify other security-related system parameters. These apply to the NetWitness Suite system and are used in conjunction with the security settings for individual services.

| What can I do here? | Path | Show me how |
|---|---|---|
| Manage hosts. | ADMIN > Hosts | See the *Host and Services Getting Started Guide*. |
| Manage services including managing service user access and security. | ADMIN > Services | See the *Host and Services Getting Started Guide*. |

| What can I do here? | Path | Show me how |
|---|---|---|
| Manage event sources and configure alerting policies for them. | ADMIN > Event Sources | See the *Event Source Management Guide*. |
| Set up and monitor alarms for the hosts and services in your NetWitness Suite domain. | ADMIN > Health & Wellness > Alarm | See the *System Maintenance Guide*. |
| Monitor statistics for the NetWitness Suite 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 Suite domain. | ADMIN > Health & Wellness > Policies | See the *System Maintenance Guide*. |
| Set global configurations for NetWitness Suite. | ADMIN > System | See the *System Configuration Guide*. |
| Configure Global Audit Logging. | ADMIN > Systen > 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*. |

# Setting up Your Default View by SOC Role

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

The following figure shows the main NetWitness Suite views.


- **Respond**: This view is for Incident Responders, who can view a list of incidents to triage and alerts. For legacy 10.6 users, this view was known as the Incident Management view and the Respond > Alerts view replaces the ESA 10.6 Alerts > Summary view .
  Respond is the default opening view. If you do not have permission to see the Respond view, you will have Monitor as your default view.
- **Investigate**: This view is for Threat Hunters, who investigate and hunt for advanced threats.
- **Monitor**: This view is for all users and it is the classic view for previous application versions. You can view dashboards and reports 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.
- **Configure**: This view is for Threat Intel (content) personnel, who configure data sources and inputs to NetWitness Suite. Threat Intel personnel use this area to download and manage Live content. They can also create and manage incident and ESA rules.
  For legacy 10.6 users, this view was Live, Incidents > Configure, and Alerts > Configure.
- **Admin**: This view is for System Administrators, who set up and maintain the overall application.

You can select any of the main NetWitness Suite views as your default view. In addition to the main views, NetWitness Suite has predefined dashboards that you can select in the Monitor 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

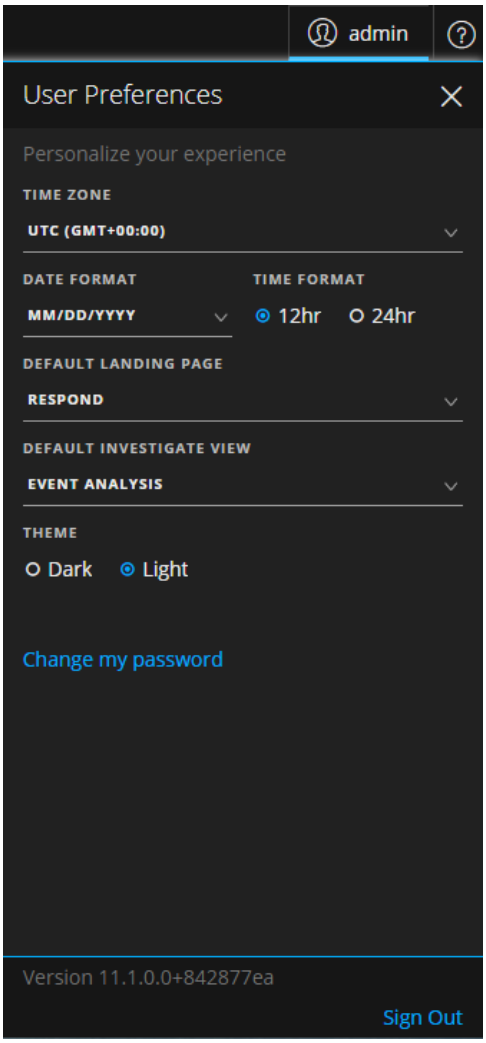
The following table shows typical SOC roles and the available views you can select as your landing page in your user preferences based on your SOC role. If you have more than one role, select the view that is most appropriate for you to start with when you log in to NetWitness Suite.

| 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 | **RESPOND** |
| Threat Hunter (Tier 2/Tier 3 Analyst) | Investigates and hunts for advanced threats | **INVESTIGATE** |
| SOC Manager (SOC Management and Reporting) | Manages SOC readiness and responds to incidents and data breaches. | **MONITOR** (Dashboard is in the MONITOR view.) 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 Suite. | **MONITOR** or **CONFIGURE** (Dashboard is in the MONITOR view. 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 MONITOR as your default view, you can navigate to the CONFIGURE view from the main menu.) |

| SOC Roles | Role Description | Consider this Default Landing Page |
|---|---|---|
| Data Privacy Officer (DPO) | Similar to an Administrator, but a DPO monitors and protects privacy-sensitive information. | **MONITOR** (Dashboard is in the MONITOR view. 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. | **ADMIN** |

## Setting Your Default View

1. (Respond view and some Investigate views) On the main menu bar, select  .
   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 Suite. Use the above table to make your selection based on your SOC role. For example, 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 Suite.

## Basic Troubleshooting Tips for User Setup

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

| Problem | Troubleshooting Tip |
|---|---|
| When I log in to NetWitness Suite, 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 MONITOR 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 Suite supports modern (or current) versions of the latest browsers. Try installing a newer browser version. If you cannot upgrade your browser, you can try<br>enabling the TLS 1.2 protocol in your browser:<br>Navigate to **Internet options > Advanced > Settings > Security**. In addition to your other protocols, ensure that the TLS 1.2 protocol is enabled. Click **Apply**. Reload the page. |
| 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 see your Administrator. |

# Setting User Preferences

You can view and manage your NetWitness Suite global application preferences from your user profile. Your global preference options vary depending on whether you access them from the Respond view or other views, such as Monitor, Configure, Admin, and Investigate.
You can:

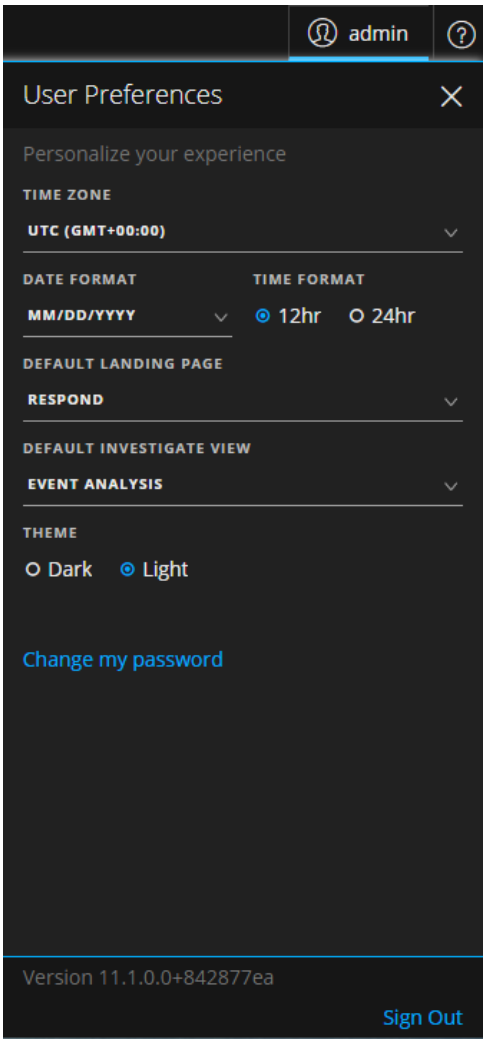
- Set the application time zone
- Set the application date and time format *
- Select your default NetWitness Suite starting location*
- Select your default Investigate view*
- Choose a dark or light theme for the application*
- Change your password (See Changing Your Password for more information.)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

* You can make this change from the **User Preferences** dialog accessible from Respond and some Investigate views: Event Analysis, Hosts, and Files.

** You can make this change from the **Preferences** dialog accessible from most views except Respond and some Investigate views: Event Analysis, Hosts, and Files.

## View Your User Preferences (Respond and some Investigate views)

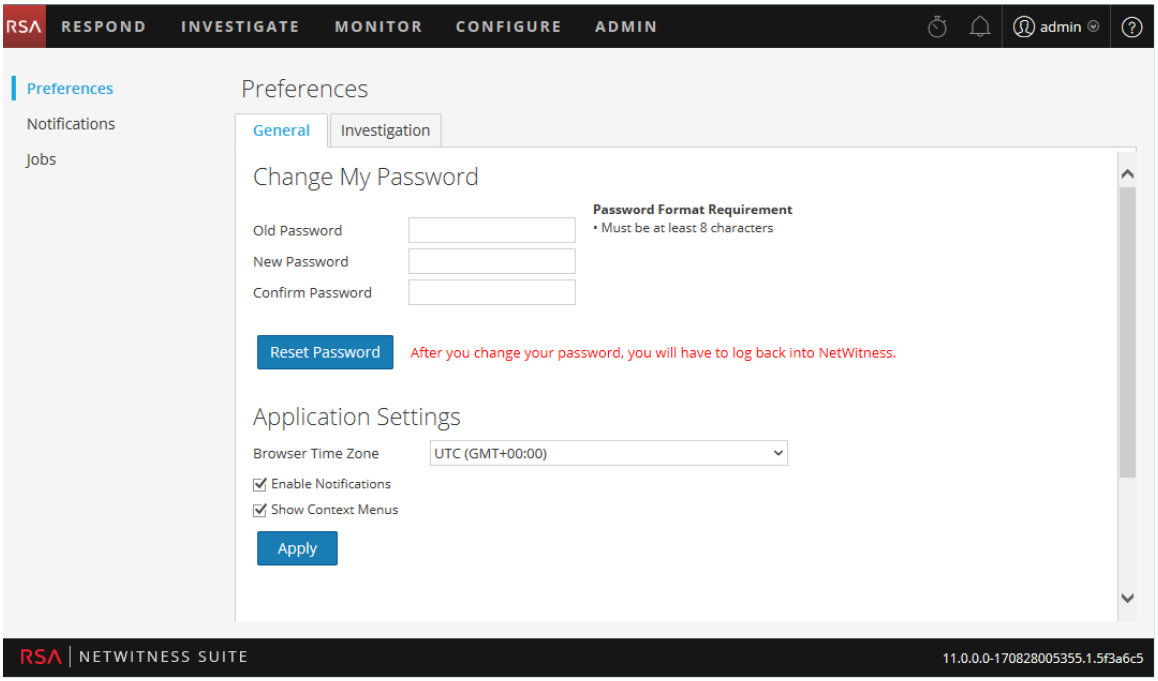
In the upper right corner of the NetWitness Suite browser window, select  .
The User Preferences dialog shows your current preferences when accessed through the Respond view and the following Investigate views: Event Analysis, Hosts, and Files.




Any selections that you make become effective immediately.

## View Your User Preferences (Most views except Respond and some Investigate views)

For most of the following views: Investigate, Monitor, Configure, and Admin: In the upper right corner of the NetWitness Suite browser window, select > **Profile**.
The Preferences dialog shows your current preferences.




## Set the Time Zone and Date and Time Format

You can change the time zone and the format of the date and time for your location.

**Note:** You can only change the date and time preferences for your location from the Respond and some Investigate views: Event Analysis, Hosts, and Files.

1. In the User Preferences dialog, select your localization preferences:
   a. **Time Zone**: Set the time zone to use in the NetWitness Suite.
   b. **(Respond and some Investigate views) 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 05/11/2017.
   c. **(Respond and some Investigate views) 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 Respond view become effective immediately.

2. **(Most views except Respond and some Investigate views)** 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 UI automatically updates to reflect the correct time.

## Select the Default NetWitness Suite Starting Location

1. **(Respond and some Investigate views)** 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 Suite. You can choose Respond, Investigate, Monitor, 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. 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. Changes become effective immediately.

## Select the Default Investigate View

1. **(Respond and some Investigate views)** Open the User Preferences Dialog.
2. In the **Default Investigate View** field, select the default landing page when you log in to NetWitness Suite and navigate to Investigate. You can choose Navigate, Events, Event Analysis, Hosts, Files, 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. See Setting up Your Default View by SOC Role to help you select the appropriate default view.

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

## Choose the Appearance of NetWitness Suite

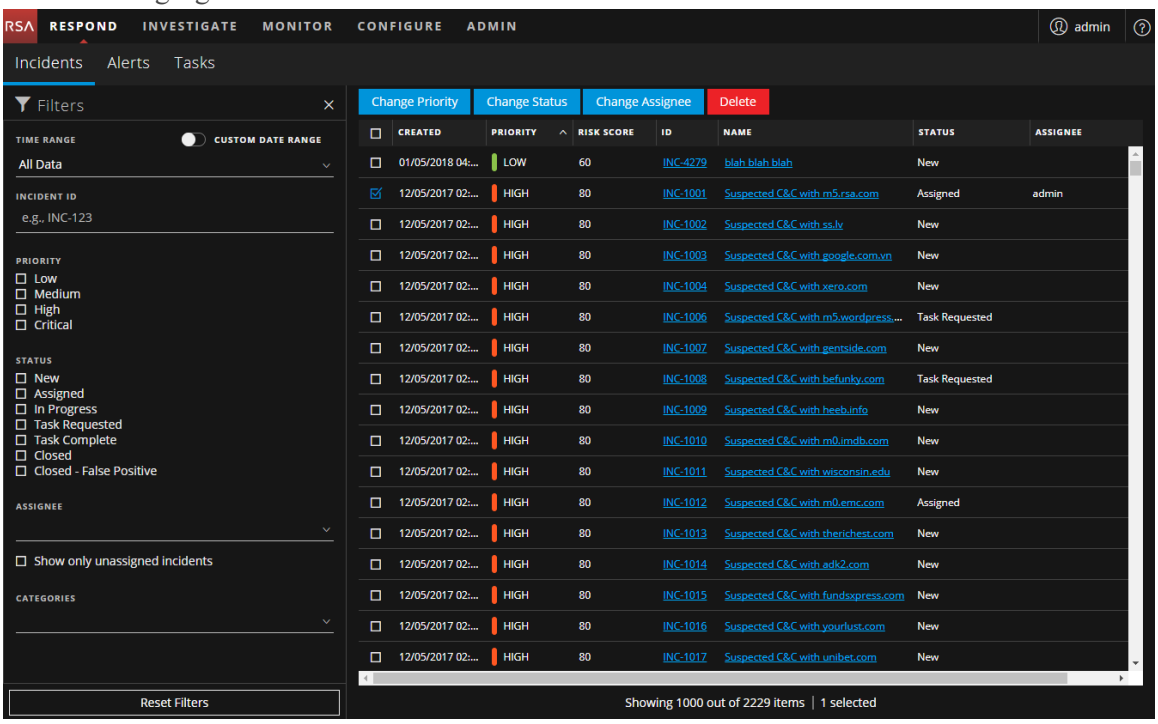
This option is only available for NetWitness Suite versions 11.1 and later.

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 Suite appears to you, not other users.

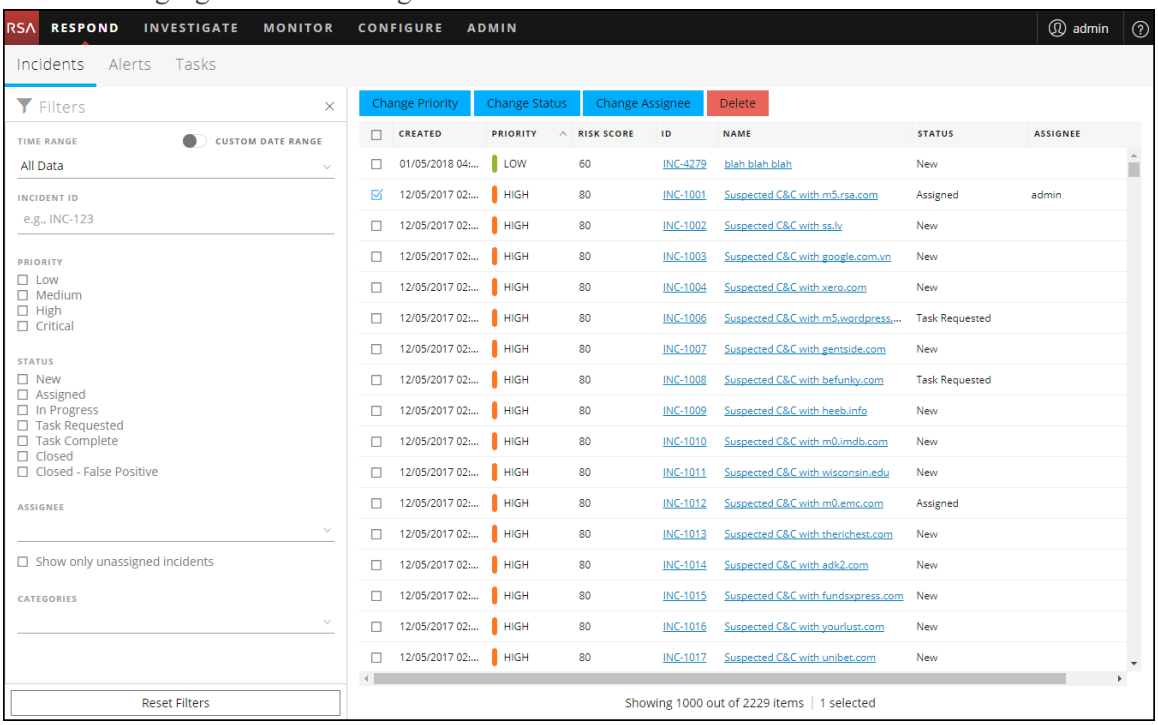
1. **(Respond and some Investigate views)** Open the User Preferences dialog.
2. Under **THEME**, select one of the following options:
   - **Dark**: The dark theme is best for darker environments or when you do not need as much contrast.
   - **Light**: The light theme is best for lighter environments,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




## Enable or Disable System Notifications for Your User Account

**(Most views except Respond and some Investigate views)** By default, NetWitness Suite 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:
   - 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

**(Most views except Respond and some Investigate views)** 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:
   - To enable context menus for your user account, select the **Enable Context Menus** checkbox.
   - To disable context menus, clear the **Enable 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*.

# Managing Dashboards

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

By default, the NetWitness Suite default dashboard is displayed when you log in to NetWitness Suite, and it is populated with a few useful dashlets to get you started with your own customizations. The dashboards for all NetWitness Suite components are available to add to the default NetWitness Suite dashboard or a custom NetWitness Suite dashboard.

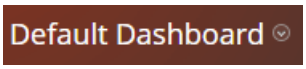
You can view dashboards and reports on different areas of interest depending on your user permissions. You have the option to select a preconfigured dashboard, import a dashboard, or create your own custom dashboard. The dashboards help you to quickly and easily view reports. You can configure your dashboards 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 Monitor view is your default landing page following logging in to NetWitness Suite you will 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 Suite component, go to **MONITOR** > **Overview**.

### 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 Suite toolbar.


A dashboard has:

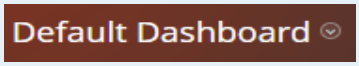
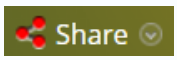
- The dashboard toolbar
- The dashboard title and the dashboard selection list.

## 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. |

| Option | Description |
|---|---|
|  | 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. |
|  | 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 Suite Suite, the following preconfigured dashboards are automatically activated and are available to you:

- Default
- Identity
- Investigation
- Operations - File Analysis
- 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:

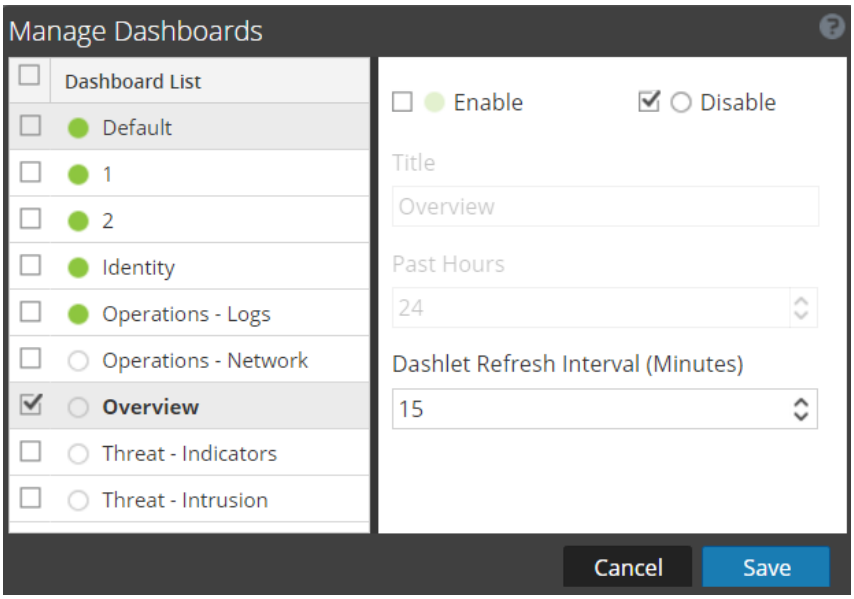
- Edit a dashboard
- Export a dashboard
- Share a dashboard
- Delete a dashboard

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.

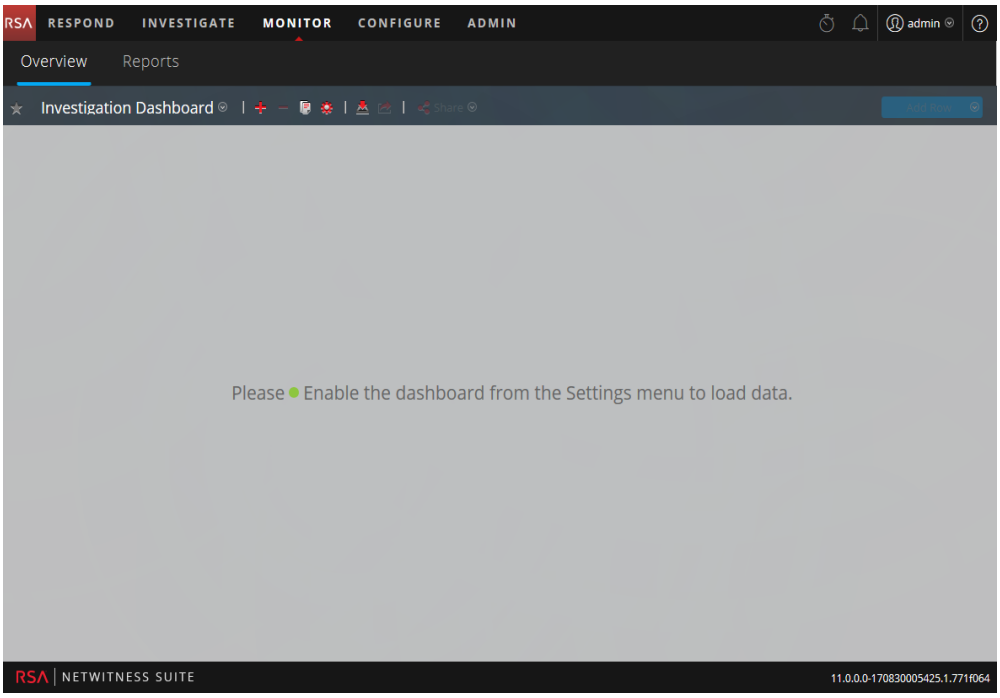
NetWitness Suite modules can display only those dashlets presented in the Manage Dashlet dialog. The main dashboard offers all NetWitness Suite dashlets. This is an example of currently available dashlets.




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

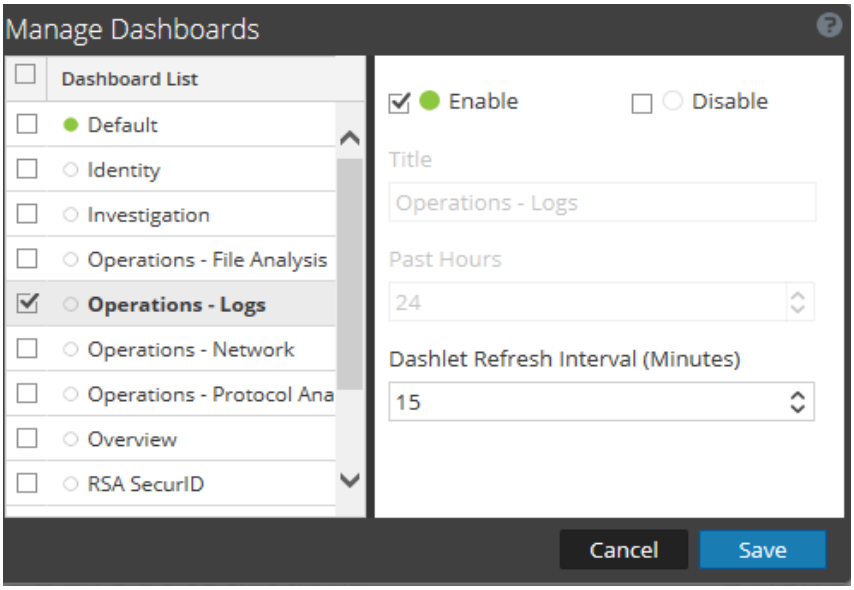
## Enabling a Dashboard

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




To enable one or more dashboard(s):

1. Navigate to the dashboard to be enabled.
2. In the dashboard toolbar, click  .
3. Select the **Manage Dashboard** option.
   The Manage Dashboards dialog is displayed.



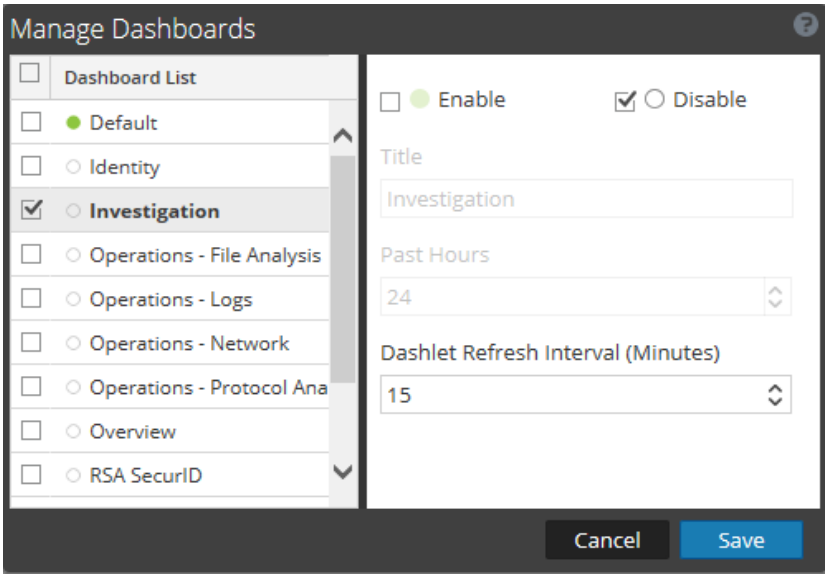

4. From the dashboard list, select the dashboard(s) to be enabled.

5. Click the **Enable** checkbox.
6. Click **Save**.

### Disabling a Dashboard

To disable one or more dashboard(s):

1. Navigate to the dashboard to be disabled.
2. In the dashboard toolbar, click  .
3. Select the **Manage Dashboard** option.
   The Manage Dashboards dialog is displayed.




4. From the dashboard list, select the dashboard(s) to be disabled.
5. Click the **Disable** checkbox.
6. Click **Save**.

## Setting a Dashboard as a Favorite

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

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.

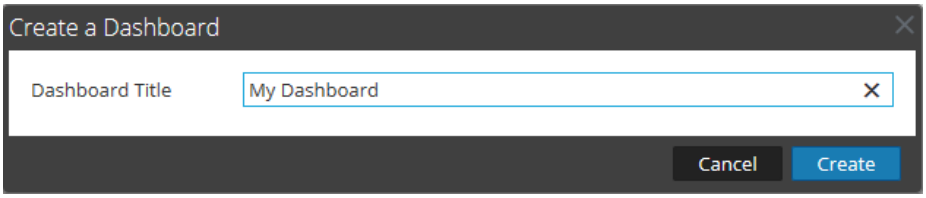
## Creating Custom Dashboards

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:

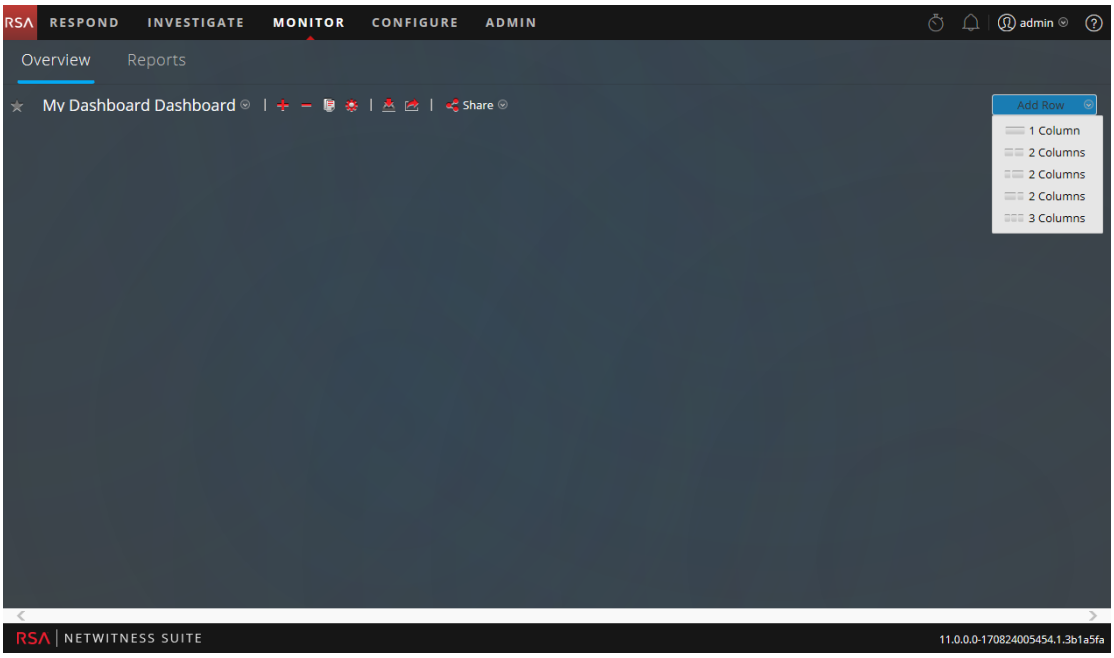
1. In the dashboard toolbar, click  .

   The Create a Dashboard dialog is displayed.



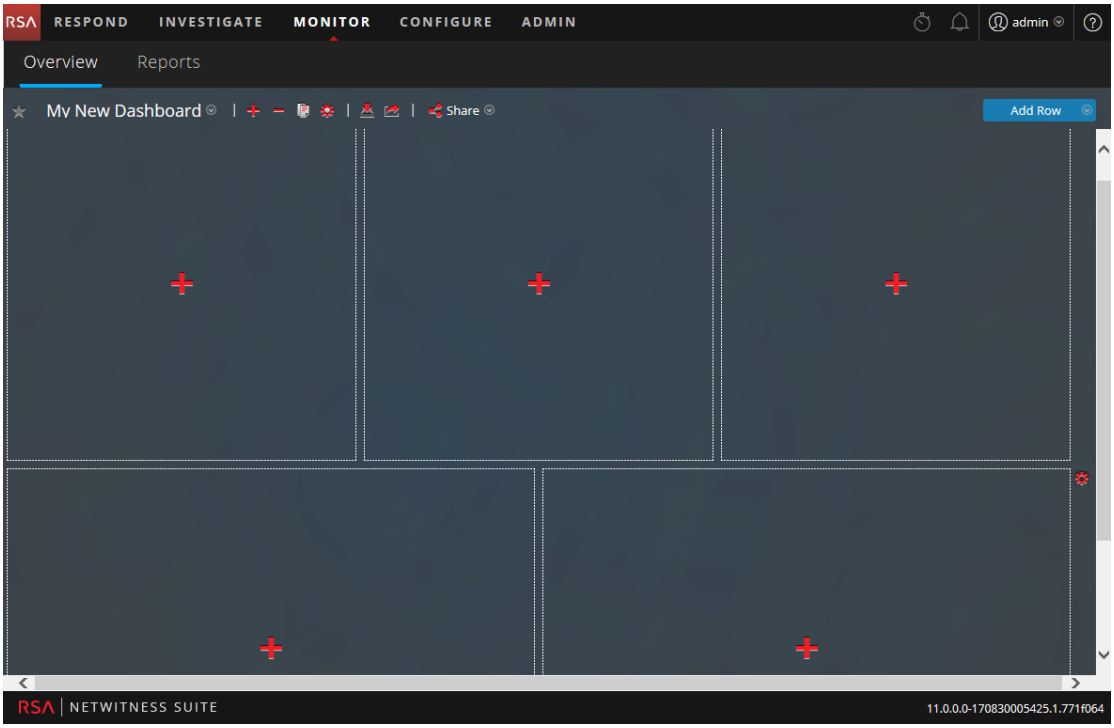

2. Enter a title for the new dashboard and click **Create**.

   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** (  ) control on the right side of the screen. Just click on 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 now add any desired dashlets to the dashboard by click the  in an empty placeholder in a row. For complete details on adding and managing dashlets, see Working with Dashlets.

Once 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

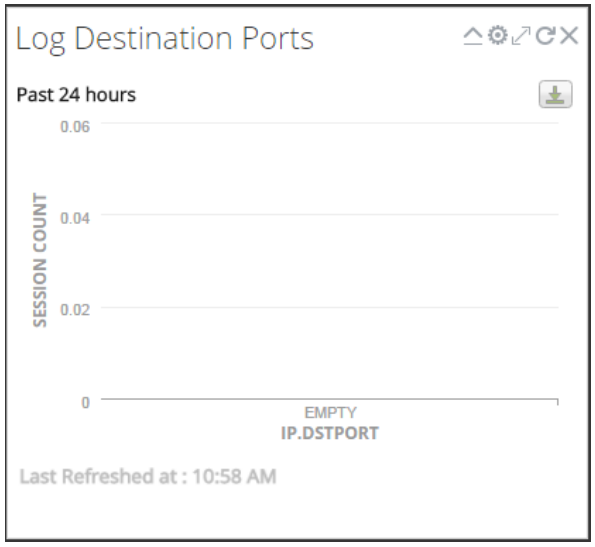
Each dashboard has:

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

## Working with Dashlets

NetWitness Suite uses dashlets to display focused subsets of system information, services, jobs, resources, subscriptions, rules, and other information.

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




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

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

| Icon | Name | Description |
|---|---|---|
| View More | | When clicked, navigates to the corresponding dashboard which is linked to the main dashlet and displays more details. If you have not linked the dashboard to an existing dashlet, this link with not be available on the dashlet. To configure this option, click  , and in the Dashboard Link field select a related dashboard view more details of the specific dashlet.<br>**Note:** This feature is only available for the realtime chart dashlet and the preconfigured dashboards in NetWitness Suite 11.0 or later. |

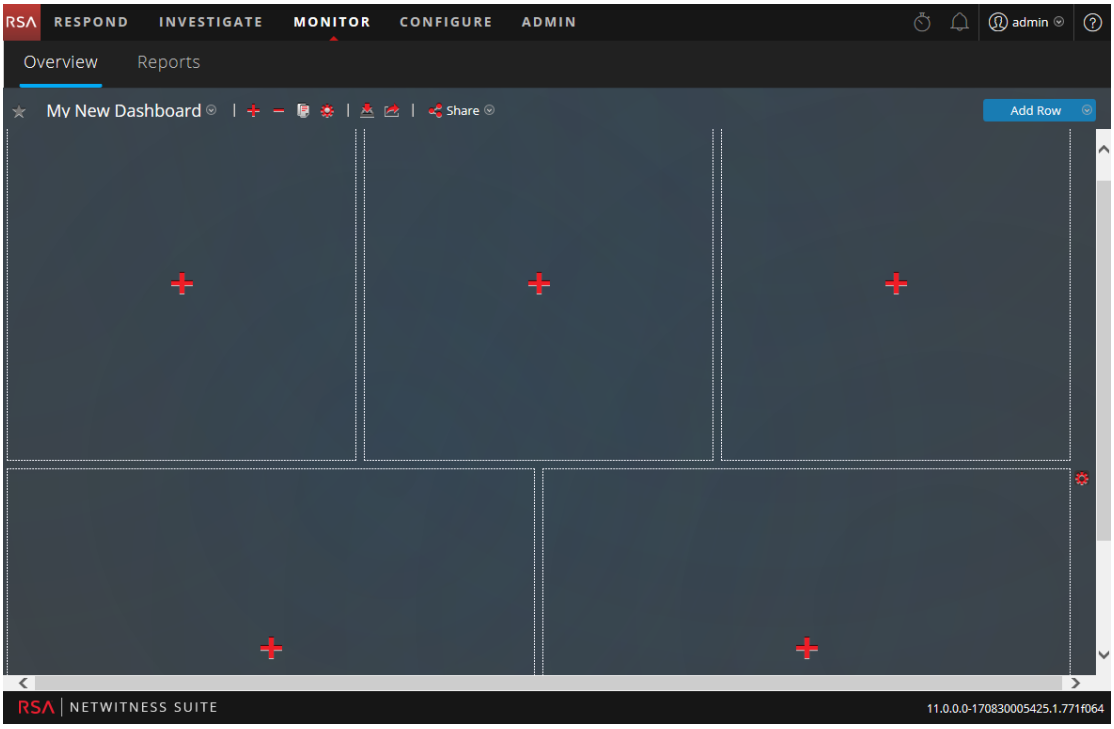
You can add dashlets to the default dashboard or construct a custom dashboard with your own useful set of dashlets to make your workflow more efficient.

## Add a Dashlet

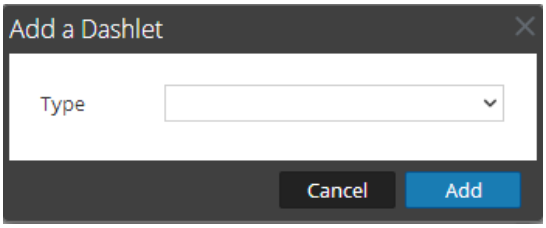
To customize the views in NetWitness Suite, you can add dashlets to a default dashboard or create custom dashboards. However, you cannot add dashlets to preconfigured dashboards.

To add a dashlet:

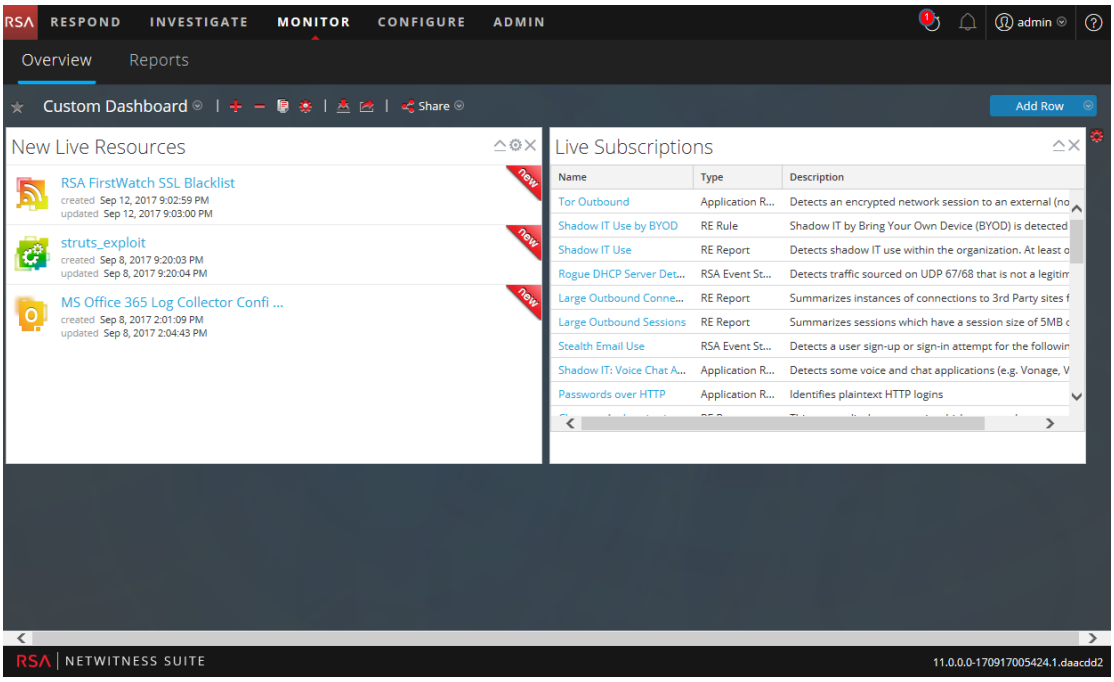
1. Navigate to any dashboard or create a new dashboard.



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




3. Click on the Dashlet **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 will be displayed 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.

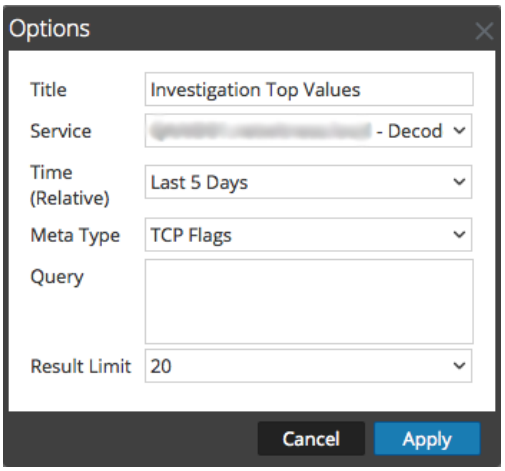
A dashlet without editable properties, such as the Live Subscriptions dashlet, does not display the settings option in the title bar. Many dashlets have an editable title where you can edit the following properties:

- 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.

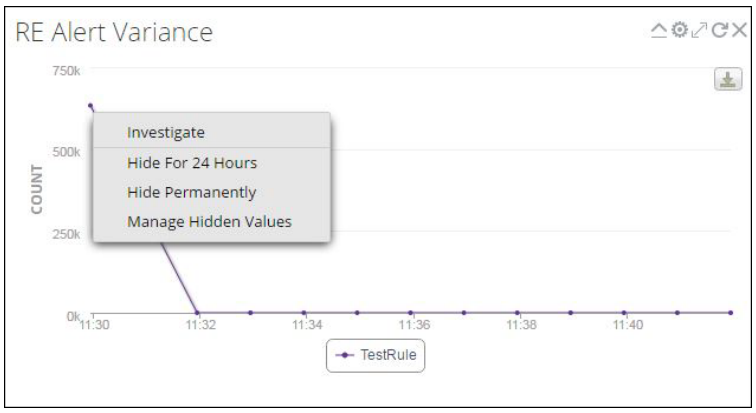



2. Edit any of the displayed properties. For example, in an Investigation Top Values dashlet, you can edit the Result Limit from 20 to 40.
3. Click **Apply**.

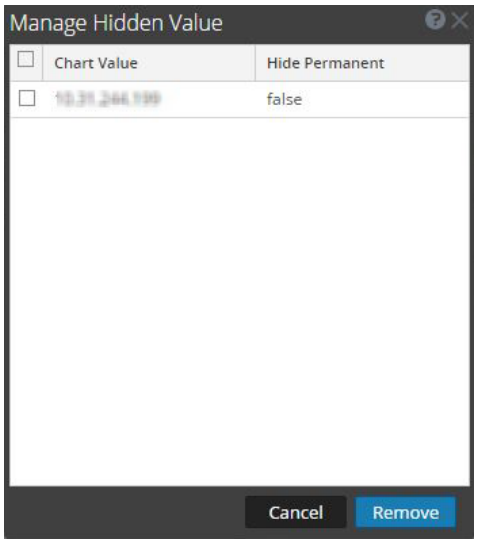
Some dashlets have configuration options to tailor the appearance or the contents of the dashlet. The following options are available for RE Top Alerts, RE Alert Variance, and RE Realtime Charts dashlets on left-click:

- **Hide For 24 Hours**: This option allows you to hide the selected value for the next 24 hours. After 24 hours, the data will automatically be 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.




**Note:** 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 will be 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 will be applicable only to your dashboard. If another user views the same overview dashboard, the value will still be 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 will still be 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

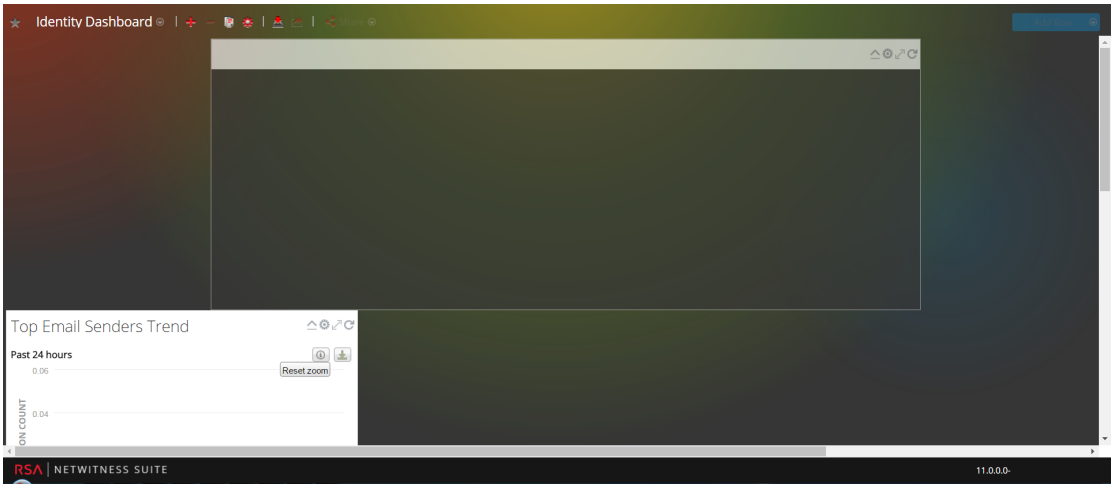
You can arrange dashlets according to your preference by dragging and dropping them into a different order on the dashboard.

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.

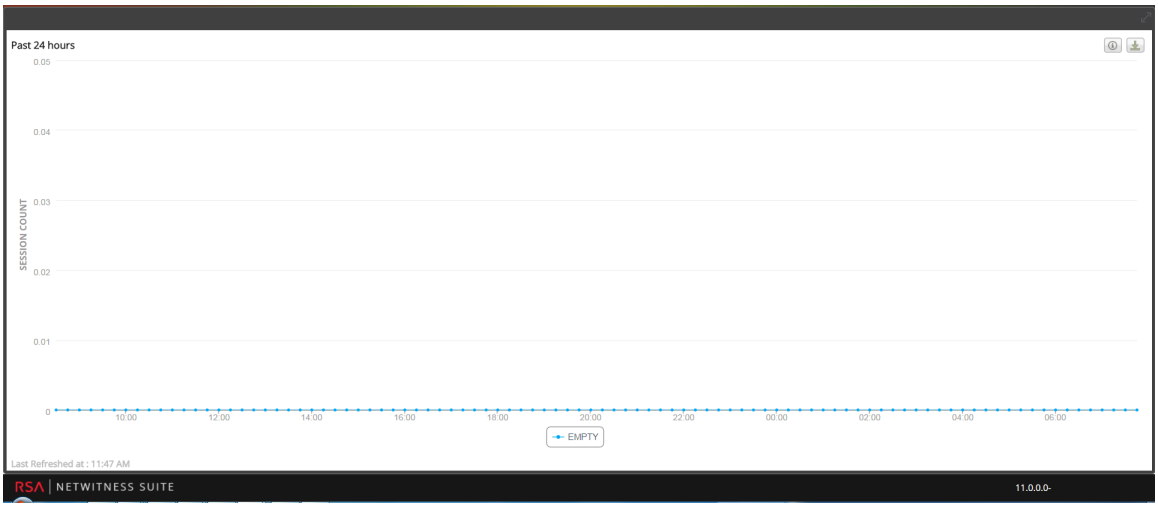
   The dashlet that currently occupies that position moves down.

## Maximize a Single Dashlet

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

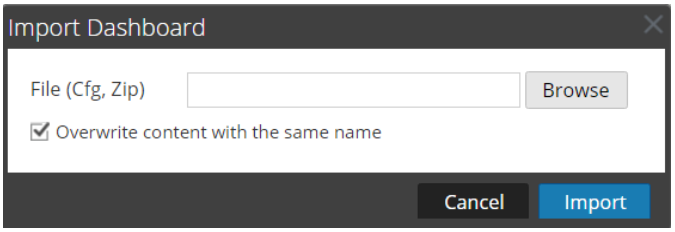
## Importing and Exporting Dashboards

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 Suite.

### Import a Dashboard

1. In the dashboard toolbar, select **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 Dashboard**.
   The dashboard is displayed in NetWitness Suite

**Note:** If you import a dashboard from Security Analytics 10.6. x into NetWitness Suite11.x, the dashboard and the associated rules and charts must be imported separately. But when you import a dashboard from NetWitness Suite11.x into NetWitness Suite, the dashboard and all the rules and charts associated with it, gets imported in .zip format.

### Export a Dashboard

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

Exported dashboards are designed to work within the same NetWitness Suite 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. Click Export Dashboard (  ) in the dashboard toolbar.
   The exported file is saved in the .zip format.

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

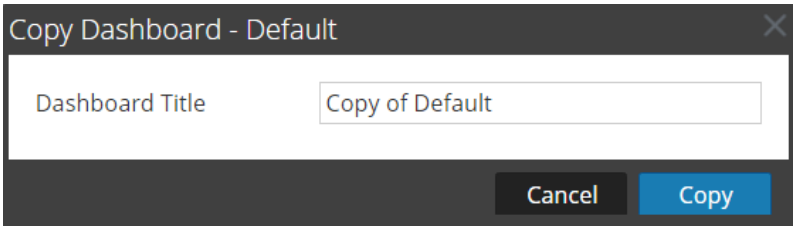
## Copying a Dashboard

To customize the views in NetWitness Suite, you can copy dashboards to the NetWitness dashboard or a custom dashboard. The NetWitness Suite dashboard, as the name suggests, offers all NetWitness Suite dashlets. The Copy Dashboard dialog creates a duplicate dashboard, which can be customized. When you copy a dashboard, the default name will be 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 - Default dialog is displayed. The following screenshot is an example

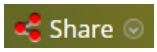
of copying a dashboard.




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

## Sharing a Dashboard

In NetWitness Suite, 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 will be able to 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.

# Managing Jobs

Inevitably, there are tasks, on-demand or scheduled, in NetWitness Suite that take a few minutes to be completed. The NetWitness Suite jobs system lets you begin a long-running task and continue using other parts of NetWitness Suite 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 Suite, you can open a quick view of your jobs from the NetWitness Suite 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.

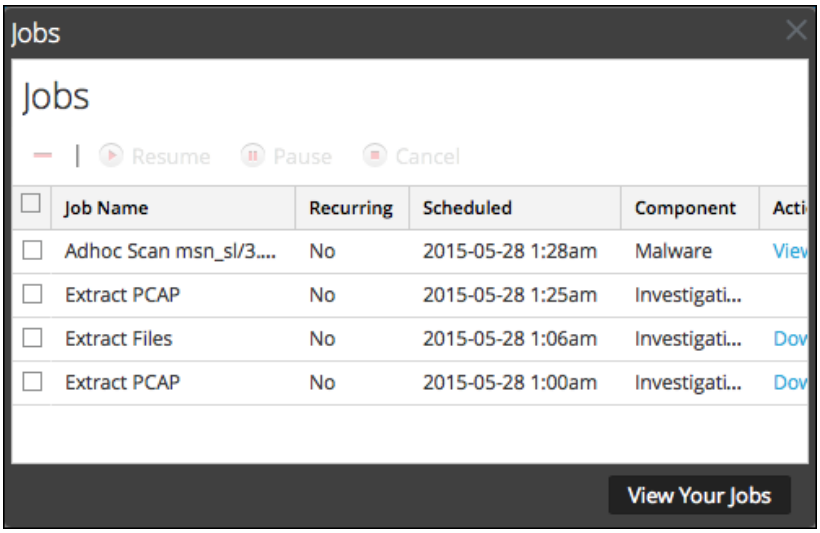
- In the Profile view, you see the same jobs in a full panel. These are only your jobs.
- In the System view, users with administrative privileges can view and manage all jobs for all users in a single jobs panel.

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

## Display the Jobs Tray

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

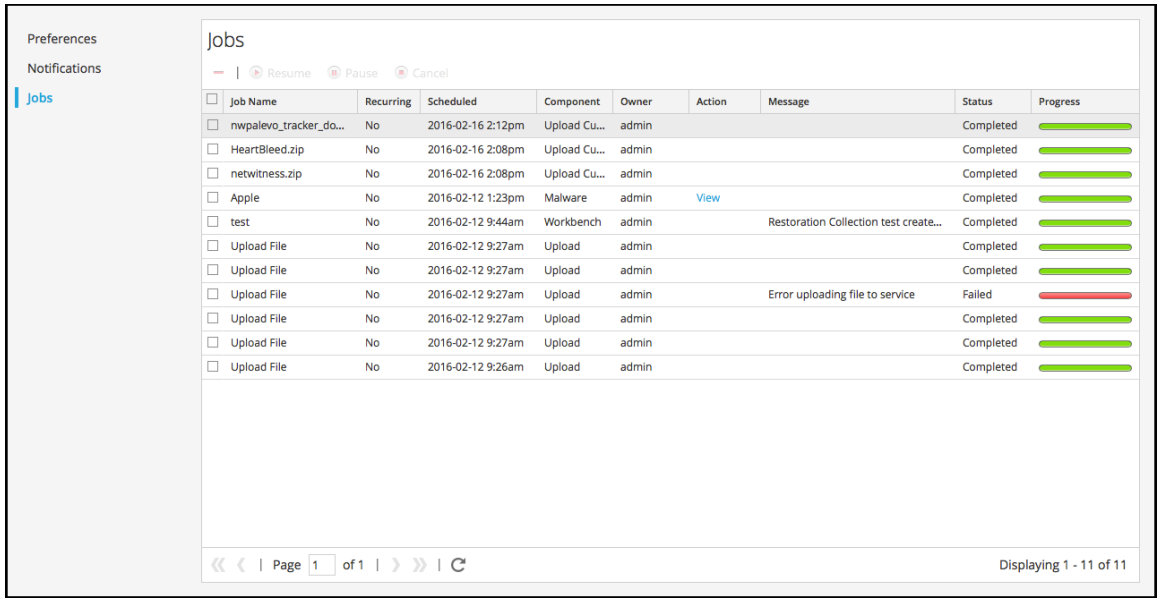
The Jobs Tray is displayed.




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 view Jobs panel are the same. In the Admin System view, the Jobs panel lists information about all NetWitness Suite jobs for all users.

## View All of Your Jobs

To see a larger view of your jobs, click **View Your Jobs**.
The Profile view > Jobs panel is displayed.



## Pause and Resume Scheduled Execution of a Recurring Job

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

1. To stop the next execution of a recurring job, in any **Jobs panel**, select the job, and click **Pause**.

   The next execution of the job is skipped, and the schedule is paused until you click Resume.

2. To restart execution of paused recurring jobs, select the job and click **Resume**.

   The next execution of the job occurs as scheduled, and the schedule for the job resumes.

## Cancel a Job

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

1. In the **Jobs Tray** or either **Jobs** panel, select one or more jobs.
2. Click **Cancel**.

   A confirmation dialog is displayed.

3. Click **Yes**.

   The jobs are canceled, and the entries remain in the grid 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 grid. 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 **Delete**.
3. The jobs are deleted from the grid.

## Download a Job

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

# Viewing and Deleting Notifications

While you are working in NetWitness Suite, you can view recent system notifications without leaving the module in which you are working. You can open a quick view of notifications from the NetWitness Suite 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.

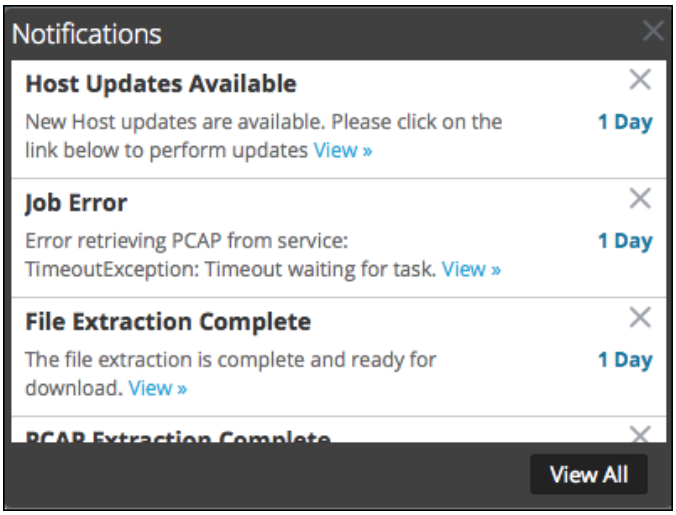
You can see notifications in these two views.

- 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 the Notifications tray, click the Notifications icon ( ).

The Notifications tray is displayed.

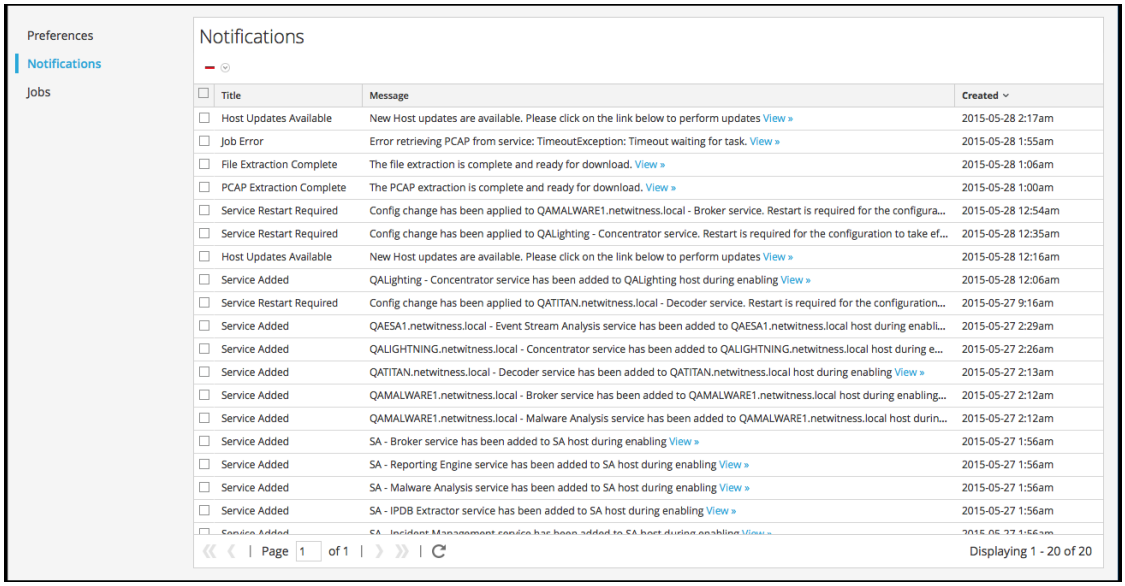


## View All of Your Notifications

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

- Click  to open the Notifications tray, then click **View All** in the Notifications tray.
- In the upper right corner of the NetWitness Suite browser window, select  > **Profile** and then 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** table, select the notifications that you want to delete.
2. Click .

   The selected notifications are deleted from this table and from the Notifications Tray.

# Viewing Help in the Application

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

## View Inline Help

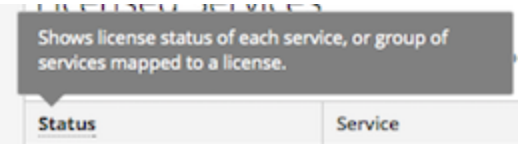
Inline help provides additional information about what to do in sections or fields that you are currently viewing in the NetWitness Suite user interface. To display inline help, hover over . The inline help shows a brief description of the element.

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:

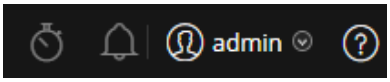



## View Online Help

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



# Finding Documents on RSA Link

The RSA NetWitness® Suite 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 Suite Documentation

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

### To navigate to NetWitness Suite Logs and Packets documentation:

1. On the RSA Link homepage (https://community.rsa.com), click **RSA NETWITNESS SUITE**.
2. On the RSA NetWitness Suite page, click **DOCUMENTATION** and select **RSA NETWITNESS LOGS AND PACKETS**.

### To navigate to NetWitness Endpoint 4.x documentation:

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

## Locate RSA Content

RSA Content is 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 SUITE**.
2. On the RSA NetWitness Suite page, click **DOCUMENTATION** and select **ADDITIONAL RESOURCES** > **RSA CONTENT**.

## Locate RSA Supported Event Sources

RSA Supported Event Sources are at the following link:
https://community.rsa.com/community/products/netwitness/parser-network/event-sources

**To navigate to RSA Supported Event Sources:**

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

## Find Documents Using NetWitness Navigator

You can search for desired RSA NetWitness Suite documentation in RSA Link using the NetWitness Navigator tool.

1. On the RSA Link homepage (https://community.rsa.com), click **RSA NETWITNESS SUITE**.
2. Under PRODUCT RESOURCES (right side of page) click **RSA NetWitness Navigator**.
3. Select desired search criteria from the available options. When searching for documentation, you should select **User Documentation** as the Content Type. Also, the Cost option is ignored for user documentation.
4. Click **VIEW RESULTS** to view a list of matching documents.
5. Click **RESET OPTIONS** to clear your previous search options.

## 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.

# NetWitness Suite Getting Started References

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

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

## User Preferences

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

- Set the application time zone
- Set the date and time formats
- Select your default NetWitness Suite 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 from the Respond view or other views, such as Investigate, Monitor, Configure, and Admin. There are two global user preferences dialogs accessible from the main menu bar:

- **User Preferences** dialog: Accessible from Respond and the following Investigate views: Event Analysis, Hosts, and Files.
- **Preferences** dialog: Accessible from most other views.

### What do you want to do?

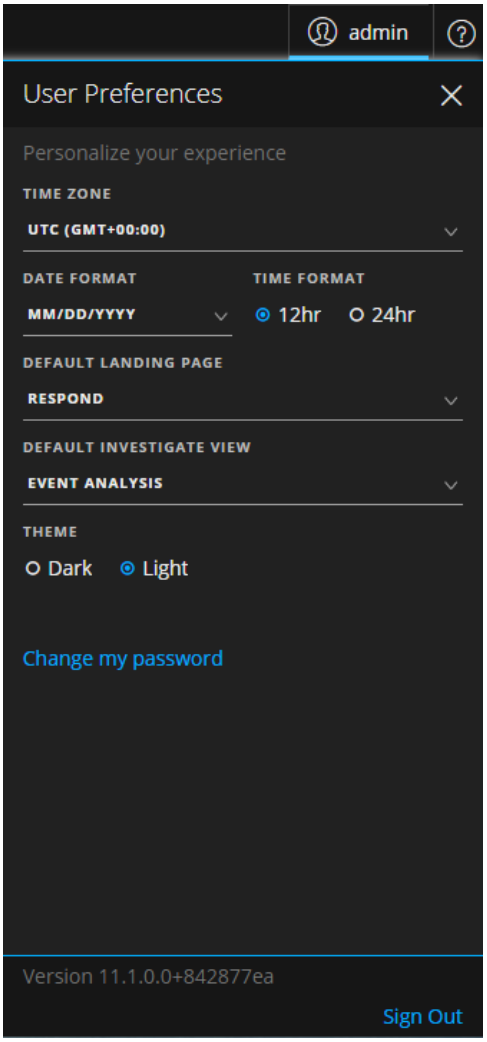
| Role | I want to ... | Show me how |
|---|---|---|
| All | Change my Password | Change My Password |
| All | Choose my Default Landing Page | Setting up Your Default View by SOC Role |
| All | Set my User Preferences | Setting User Preferences |

### Related Topics

- NetWitness Suite Basic Navigation

## User Preferences (Respond and some Investigate views)

To access your user preferences, click .
The User Preferences dialog shows your current preferences and the NetWitness Suite version.




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

| Option | Description |
|---|---|
| Time Zone | Sets the time zone to use in NetWitness Suite. |
| 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. |

| Option | Description |
|---|---|
| Time Format | Sets the time as 12-hour or 24-hour time. For example, 2:00 PM in 12-hour time is 14:00 in 24-hour time. |
| Default Landing Page | Enables you to select the default view when you log in to NetWitness Suite. You can choose Respond, Investigate, Monitor, 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.<br>This selection sets the default view for the entire application. |
| Default Investigate View | (This option applies to NetWitness Suite 11.1 and later.) Select the default landing page for the Investigate view. You can choose Navigate, Events, Event Analysis, Hosts, Files, 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 Suite 11.1 and later.)<br>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:<br>• **Dark**: The dark theme is best for darker environments or when you do not need as much contrast.<br>• **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.<br>Your selection only changes how NetWitness Suite appears to you, not other users. |
| Change my password | Opens the Preferences dialog where you can change your password. |
| Version | Shows the NetWitness Suite version. |
| Sign Out | Enables you to log out of NetWitness Suite. |

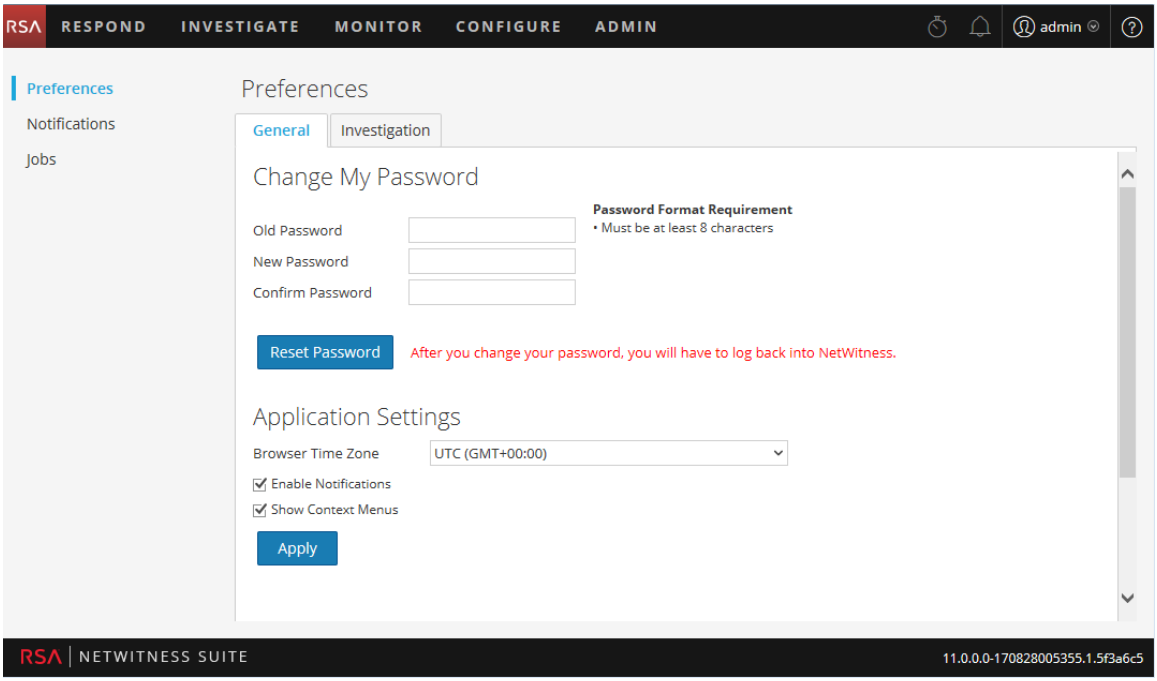
Any selections that you make become effective immediately.

## Preferences

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

- For most views, such as Investigate, Monitor, Configure, or Admin, go to > **Profile**.
- In the Respond and some Investigate views (Event Analysis, Hosts, and Files), select 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

This section enables you to change your password. Your Administrator defines the appropriate password strength requirements for your NetWitness Suite 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 Suite. |

| Option | Description |
|---|---|
| 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 Suite for the changes to take effect. The new password becomes effective the next time you log in to NetWitness Suite. The password change is applied to your system login and to all NetWitness Suite services on which your account has been added. |

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

#### Application Settings

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

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

## Notifications Panel and Notifications Tray

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

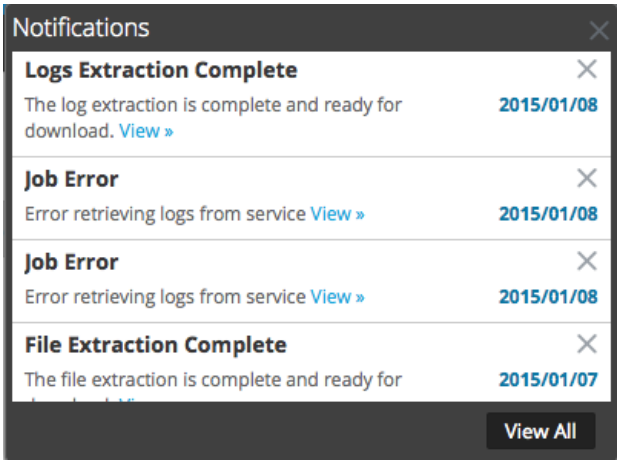
When you are viewing notifications in the Notifications tray, only recent notifications are displayed. You can access all of your notifications from your user Profile and from the Notifications tray by selecting the View All option. Procedures for viewing notifications are provided in Viewing and Deleting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

### What do you want to do?

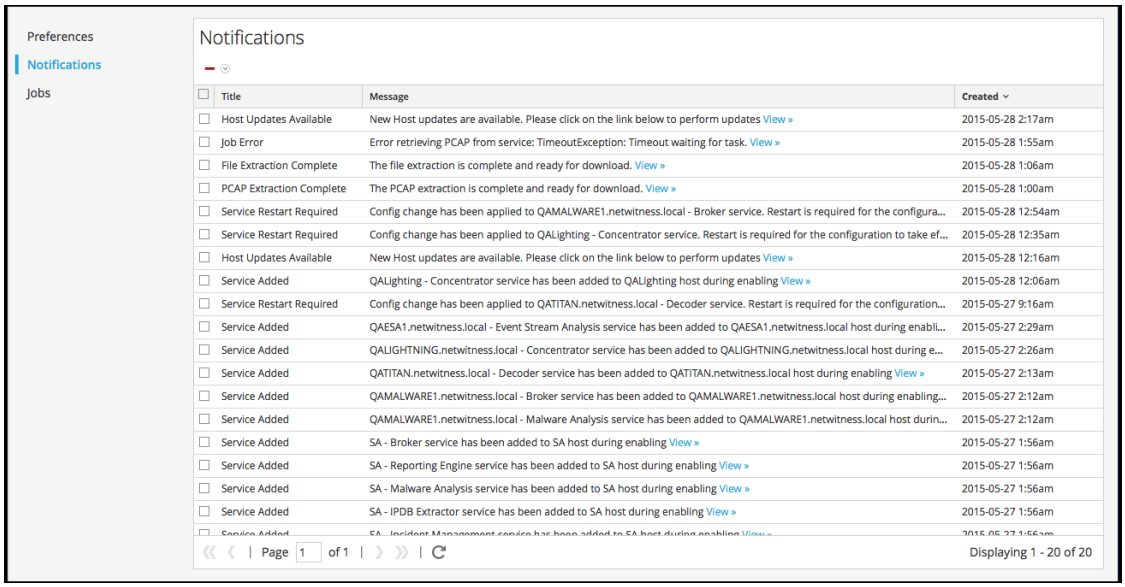
| Role | I want to ... | Show me how |
|---|---|---|
| All | View all notifications | Viewing and Deleting Notifications |
| All | Delete notifications | Viewing and Deleting Notifications |

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 Suite browser window, select  > **Profile** and then 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, **File Extraction Complete**. |
| **Message** | The entire message, for example, **The file extraction 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.<br>In the Notifications Tray, this column is the number of days since the notification was created. |
| **View All** | (Notification tray only) Opens the Notifications panel, which lists all of your notifications. |

## Jobs Panel and Jobs Tray

Jobs are started by various NetWitness Suite modules; for example, the Live module can download CMS resources, the Administration module can upload a feed to a service, and the Investigation module can analyze and reconstruct packets in packet capture files.

In the Administration System view, users in the ADMIN group can manage all NetWitness Suite jobs in the Jobs panel. Other non-administrative users can view their own jobs in the Profile view.

In addition, while working in NetWitness Suite, you can open a quick view of your jobs from the NetWitness Suite 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

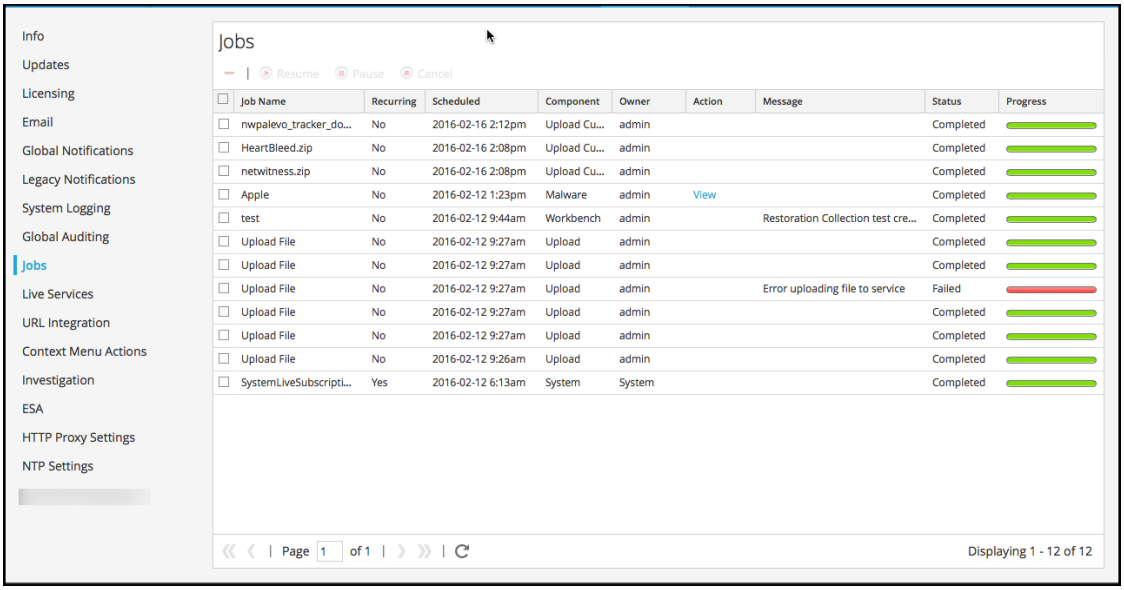
The structure of the jobs panel is the same in all views.

### What do you want to do?

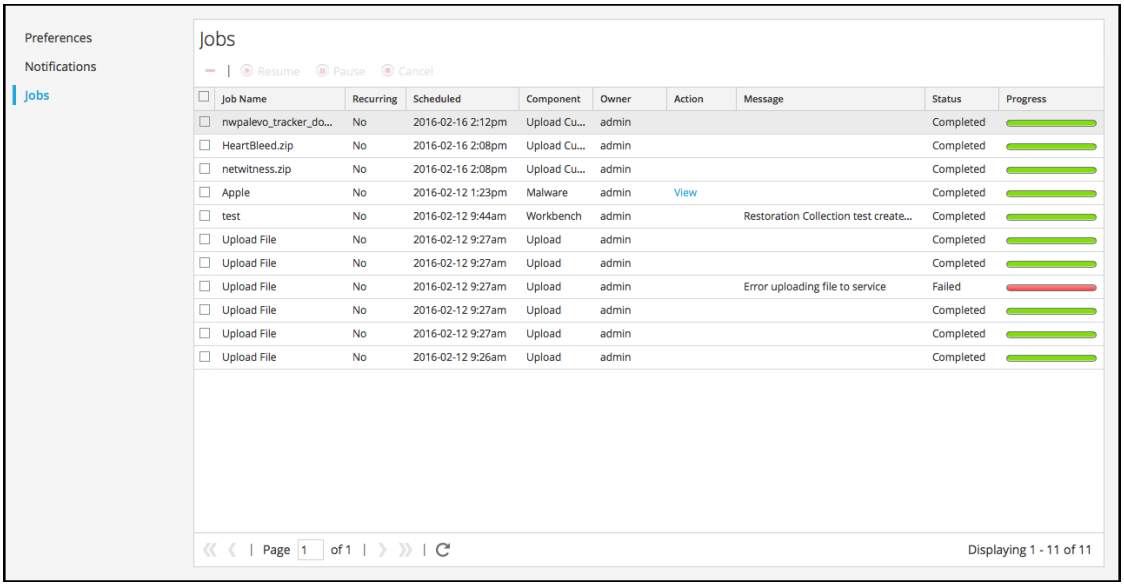
| Role | I want to ... | Show me how |
|---|---|---|
| All | Pause and Resume a Scheduled Job | Managing Jobs |
| All | Cancel or Delete a Job | Managing Jobs |
| | Download a Job | Managing Jobs |

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

- Go to **ADMIN > System**, and in the options panel, select **Jobs**.

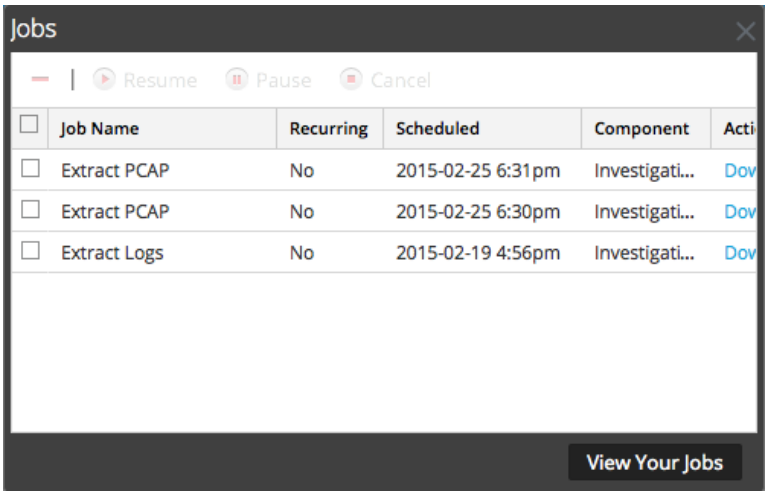



- Go to **Profile**, and in the options panel, select **Jobs**.




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 Suite module 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 Profile view > Jobs panel are the same. In the Admin System view, the Jobs panel lists information about all NetWitness Suite jobs for all users.

The following table describes the options in the Jobs panel.

| Feature | 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. |

| Feature | Description |
| --- | --- |
|  | 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 features.

| Feature | Description |
| --- | --- |
| Selection box | Click in this box to select one or more jobs. |
| Progress | Shows the percentage complete for a job. |
| 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. |
| 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. |
| Status | Indicates the status of the job. Common values for status are **Paused**, **Running**, **Canceled**, **Failed**, **Completed**, and other status values are possible. |
| Message | Displays additional information about the job; for example, **Extracting files** or **No sessions found.** |

| Feature | Description |
| --- | --- |
| Action | Views job in the Investigation Malware Analysis 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. |
| View Your Jobs | (Jobs tray only) Displays jobs in the **Jobs panel**. |
| Scheduled | Indicates the date and time at which the job was scheduled to begin. |