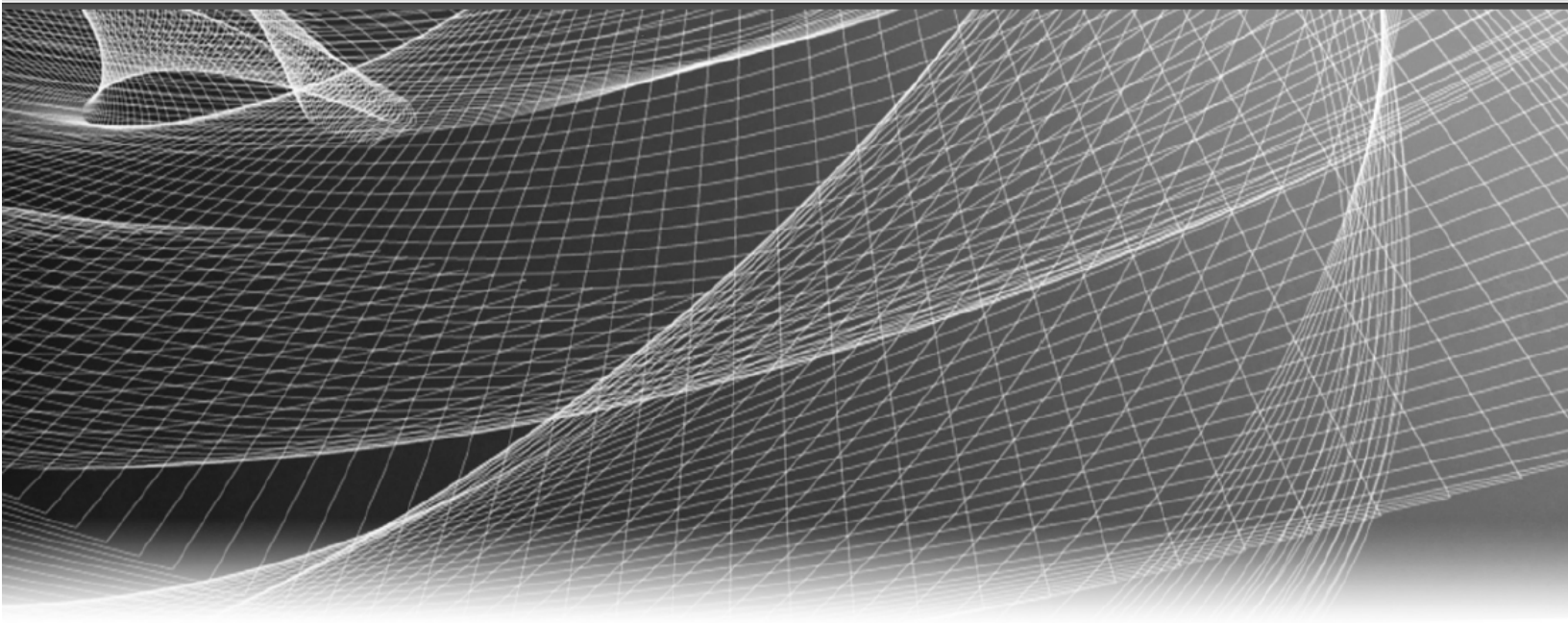


RSA | Security Analytics

Security Analytics Getting Started Guide

for Version 10.6.5

RSA

EMC²

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

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

October 2017

Contents

Getting Started with Security Analytics: Introduction to Security Analytics

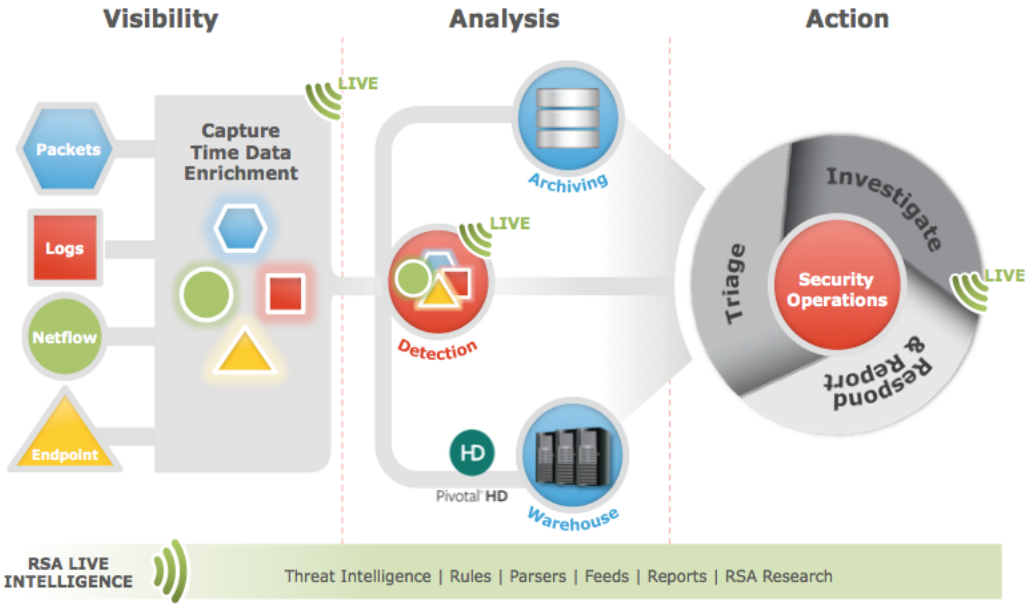
RSA Security Analytics is a distributed and modular system that enables highly flexible deployment architectures that scale with the needs of the organization. Security Analytics allows administrators to collect two types of data from the network infrastructure, packet data and log data. The key aspects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

- **Distributed Data Collection**. The packet data is collected using a host called **Decoder**, while the **Log Decoder** collects log events. The Decoder captures, parses, and reconstructs all network traffic from Layers 2 - 7, or log and event data from hundreds of devices and event sources and event sources. 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 Analytics**. The Security Analytics **Event Stream Analysis (ESA)** host 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 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.

  RSA Analytics Warehouse. A Hadoop-based distributed computing system, which collects, manages, and enables analytics and reporting on longer-term sets of security data, for example, months or years. The Warehouse can be made up of three or more nodes depending on the organization's analytic, archiving, and resiliency requirements.

  Security Analytics Server. Hosts Reporting, Investigation, Administration, and other aspects of the user interface. Also enables reporting on data held in the Warehouse.
- **Capacity**. Security Analytics 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.

Security Analytics 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 Security Analytics system has been optimized to run on virtualized infrastructure. The following image illustrates the Security Analytics Functional architecture:



The System Architecture comprises these major components: Decoders, Brokers and Concentrators, Archivers, ESA, Warehouse Connectors, RSA Warehouse. Security Analytics 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 Security Analytics Server.
- In a forensics implementation, the base configuration requires these components: Decoder, Concentrator, Broker, ESA, and Malware Analysis. An optional component is the Incident Management service, which resides on the ESA system and is used to prioritize alerts.

The table provides a synopsis of each major component:

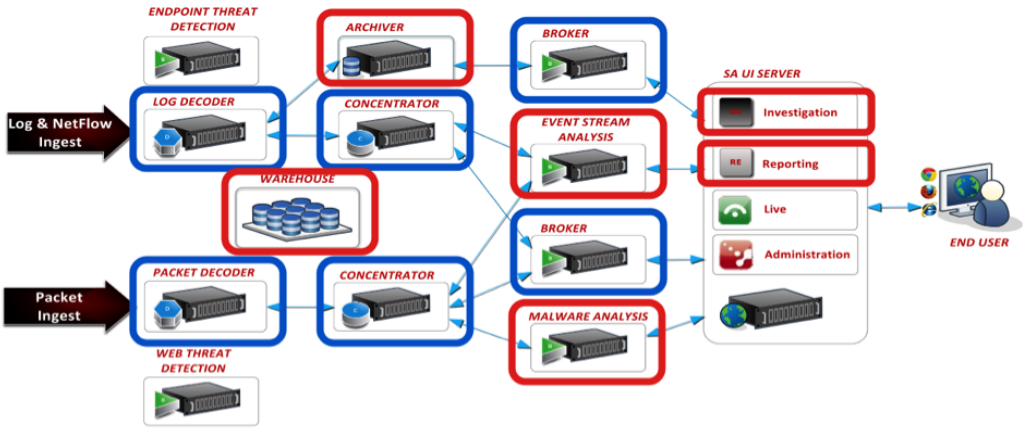
System Component	Description
Decoder / Log Decoder	• Security Analytics collects two types of data: packet data and log data. • Packet data, that is, network packets, are collected using the Decoder through the network tap or span port, which is typically determined to be an egress point on an organization's network. • A Log Decoder can collect four different log types - Syslog, ODBC, Windows eventing, and flat files. • Windows eventing refers to the Windows 2008 collection methodology and flat files can be obtained via SFTP. • Both types of Decoders ingest raw transactional data that is enriched, closed out, and aggregated to the warehouse or other Security Analytics components. • The process for ingesting and parsing transactional data is a dynamic and open framework.
Concentrator / Broker	• Any data that can be indexed on the Decoder is filtered by the respective Concentrator. • Once data is stored in the Concentrator, it is streamed as metadata to the RSA Analytics Warehouse.
Archivers	• The Archiver is a host that enables long-term log archiving by indexing and compressing log data and sending it to archiving storage. • The archiving storage is optimized for long-term data retention, and compliance reporting. • Archiver stores raw logs and log meta data from Log Decoders for long term-retention, and it uses Direct-Attached Capacity (DAC) for storage. **Note:** Raw packets and packet meta data are not stored in the Archiver.

System Component	Description
Event Stream Analysis (ESA)	• This ESA host 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. • ESA uses advanced Event Processing Language that allows users to express filtering, aggregation, joins, pattern recognition, and correlation across multiple disparate event streams. • ESA helps to perform powerful incident detection and alerting.
Warehouse Connectors	• Warehouse Connector allows you to collect meta data and events from Decoders and write them in Avro format into a Hadoop-based distributed computing system. • You can set up Warehouse Connector as a service on existing Log Decoders or Decoders or it can be run as a virtual host in your virtual environment. • The Warehouse Connector contains the following components: Data Source, Destination, and Data Stream.
RSA Analytics Warehouse	• RSA Analytics Warehouse provides the capacity for longer term data archiving through a Hadoop-based distributed computing system that collects, manages, and enables analytics and reporting on security data. • RSA Analytics Warehouse requires a service called Warehouse Connector to collect meta data and events from Decoder and Log Decoder and write them in Avro format into a Hadoop-based distributed computing system. • Any incoming data at the Log Decoder and Concentrator is ultimately forwarded to the Warehouse. • A Warehouse typically consists of two units: Storage nodes and Direct Attached Capacity (DAC). • Entire data (not just meta data) is stored in the RSA Analytics Warehouse and is available to Security Analytics when required.

Core Versus Downstream Components

In Security Analytics, the Core services ingest and parse data, generate meta data, and aggregate generated meta data with the raw data. In the figure below, the Core services are highlighted in blue; they 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 Security Analytics Core services. The downstream systems are highlighted in red; they are Archiver, Warehouse, ESA, Malware Analysis, Investigation, and Reporting.

Although the Security Analytics 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 and packet data. Investigation 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.



Security Analytics User Interface

At a very high level, Security Analytics performs two functions:

- Provides a graphical browser-based user interface to administer the Security Analytics architecture, setup configurations and permissions for services.
- Acquires the data from the Warehouse, Decoders and Concentrators, performs analysis, and runs alerts and reports.
- All Security Analytics modules share a common approach to presenting data and configuration options using a series of dashboards, views, grids, and dialogs. This helps users to navigate in a seamless and easily understandable way. Once familiar with the user

interface, users can further improve their productivity by creating custom dashboards for specific purposes. For example, a set of custom dashboards can present information for different regions or different types of threats.

Security Analytics Modules

Security Analytics organizes administrative, analytical, and reporting tasks into modules representing logical groupings of functions and tasks for services:

- The dashboard is the entry point for all Security Analytics modules, providing a portal into functions of other modules for user convenience.
- The Administration module is the user interface for administering and monitoring hosts, devices and event sources, and services. When configured, hosts, devices and event sources, and services are available to other Security Analytics modules.
- The Investigation module is the user interface that allows visualization of packets captured by Security Analytics hosts. Malware Analysis is the user interface for automated malware analysis.
- The Live module is the user interface to access and manage resources available to customers through the Live Content Management System.
- The Reports and Alerts modules provide the user interface for automated reporting and alerting functions.
- The Incidents module provides the Incident Management function in Security Analytics. The incident management function is an easy way to track the incident response process and provides the following capabilities:
  - Track the Incident Response in a consistent way.
  - Automate the process of creating actionable security incidents from incoming alerts.
  - Provide business context and investigational tools to help the team discover the root causes.
  - Track the remediation process in an automated way by integrating with a third party help desk system.
  - Track the Incident Response in a consistent way.
  - Automate the process of creating actionable security incidents from incoming alerts.
  - Provide business context and investigational tools to help the team discover the root causes.

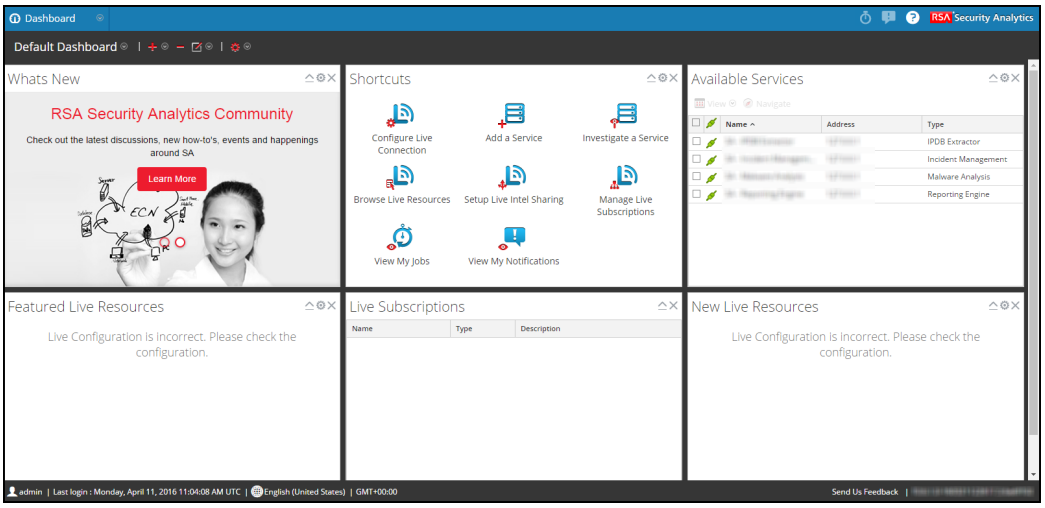
- Track the remediation process in an automated way by integrating with a third party help desk system.

Common Elements in a Browser Window

Security Analytics contains some some basic elements in every browser window. These features are included in all views of Security Analytics.

To display this view, do one of the following:

- Log on to Security Analytics at **https://<SA-IP>**, where <SA-IP> is the Security Analytics server IP address.
- In the **Security Analytics** menu, select **Dashboard**.



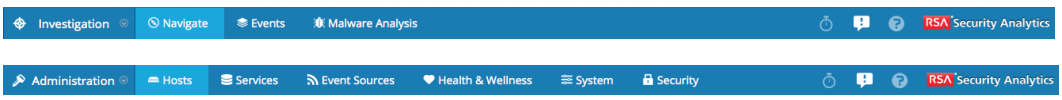
Features

Every browser window that is accessing Security Analytics includes these elements:

- The Security Analytics menu
- The Security Analytics toolbar
- The footer

Security Analytics Toolbar

At the top of all Security Analytics dashboards is the Security Analytics toolbar. Different modules have different content based on available views. Here are two examples of the Security Analytics toolbar.

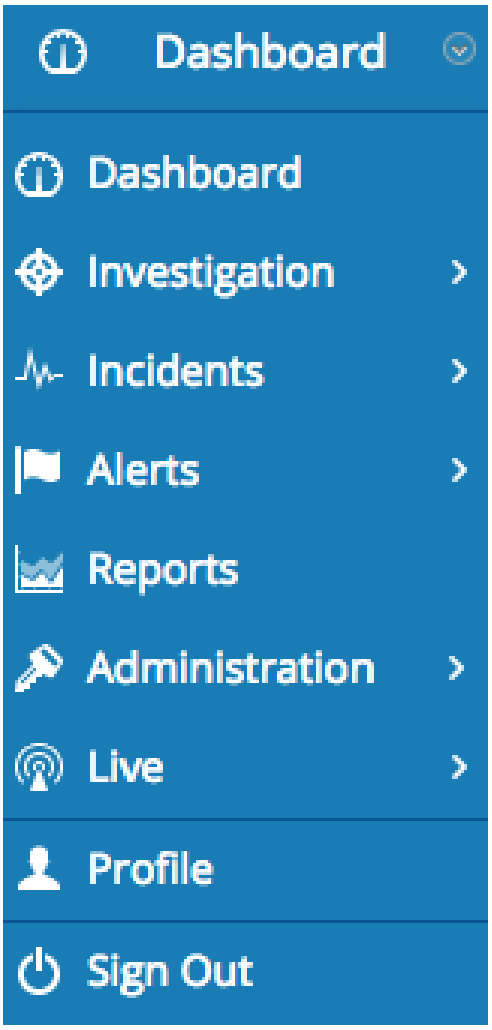


These are the features of the Security Analytics toolbar.

Feature	Description
Security Analytics Menu	Contains options to access modules, Help, Profile, and Sign Out. Some modules have a submenu of views.
Module View options	Displays a view. The option for the currently displayed view is highlighted.
Security Analytics menu	Displays the current module as the title. Click to open a drop-down menu from which you can view a module, view the Profile, or sign out of Security Analytics.
Jobs button 	Displays the Jobs tray, which provides information on jobs for a user.
Notifications button 	Displays the Notifications tray, which provides notifications for a user.
Help button 	Displays the online help for Security Analytics.

Security Analytics Menu

The Security Analytics menu is on the left side of the Security Analytics toolbar.



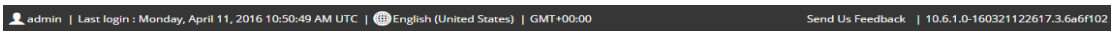
These are the options in the Security Analytics menu.

Menu Option	Description
Dashboard	Displays the Security Analytics Dashboard.
Investigation	Displays the Investigation module with the Navigate view open. The submenu has an option to display the Navigate view, the Events view, and the Malware Analysis view.
Incidents	Displays the Incident Management module. The submenu has an option to display the Queue view, Alerts view, Remediation view, and Configure view
Alerts	Displays the Alerts module with the Configure view open. The submenu has options to directly access the views: Summary and Configure.

Menu Option	Description
Reports	Displays the Reports module with the Reports view open.
Administration	Displays the Administration module with the Services view open. The submenu has options to directly access the Administration views: Hosts, Services, Event Sources, Health & Wellness, System, or Security.
Live	Displays the Live module with the Configure view open. The submenu has options to directly access the Live views: Search, Configure, and Feeds.
Profile	Displays the Profile to configure user preferences, and view notifications and jobs.
Sign Out	Signs out of Security Analytics.

Footer

The page footer is at the bottom of the browser window.



The footer provides the following information:

- The username of the logged on user
- The last login date and time of a user
- The current Security Analytics version
- The set time zone
- The set language

Send Us Feedback

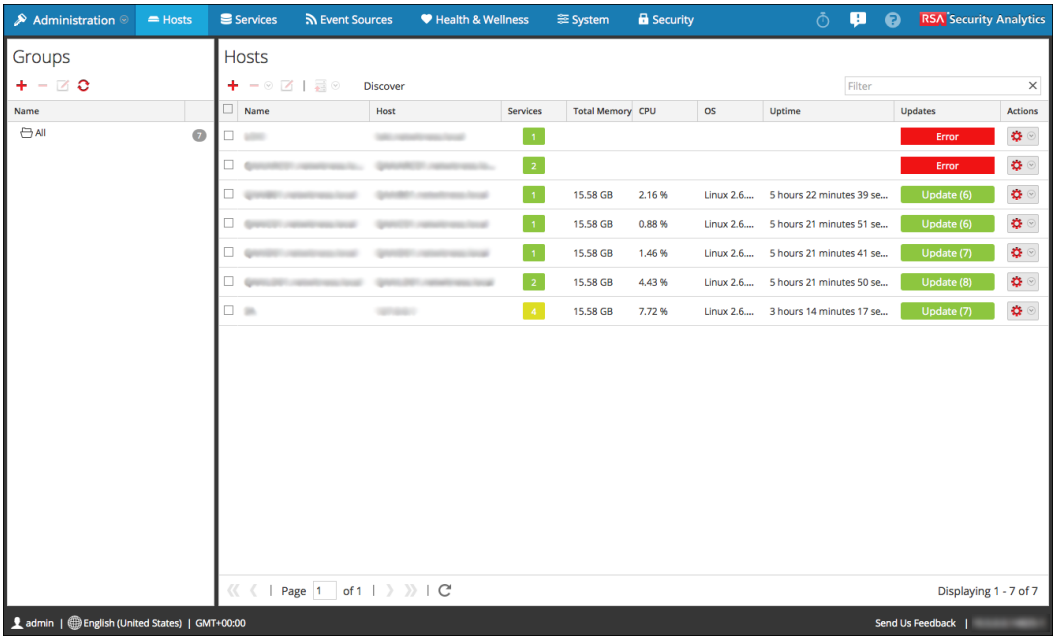
The Send Us Feedback option opens a new email message addressed to our feedback center. We appreciate your comments and suggestions, and consider them an integral part of our new features and improvements process in Security Analytics.

Common Elements in a View

The Security Analytics modules that are listed in the Security Analytics menu (Administration, Investigation, Live, Alerts, Reports, more) are called views, and each view provides functions tailored for the module. In addition, there is a Profile view, accessible directly from the Security Analytics menu, which presents options for user preferences.

To display a view, select a module from the **Security Analytics** menu. For example, **Security Analytics, Administration**, **Investigation**, or **Live**. As you roll your cursor over the module, you can select a view from the options menu. From within the module, you can select an alternate view from the Security Analytics toolbar. For example, **Administration** has six views: **Hosts, Services, Event Sources, Health & Wellness, System, and Security**.

This example of the Administration Hosts view illustrates some of the features of a view.



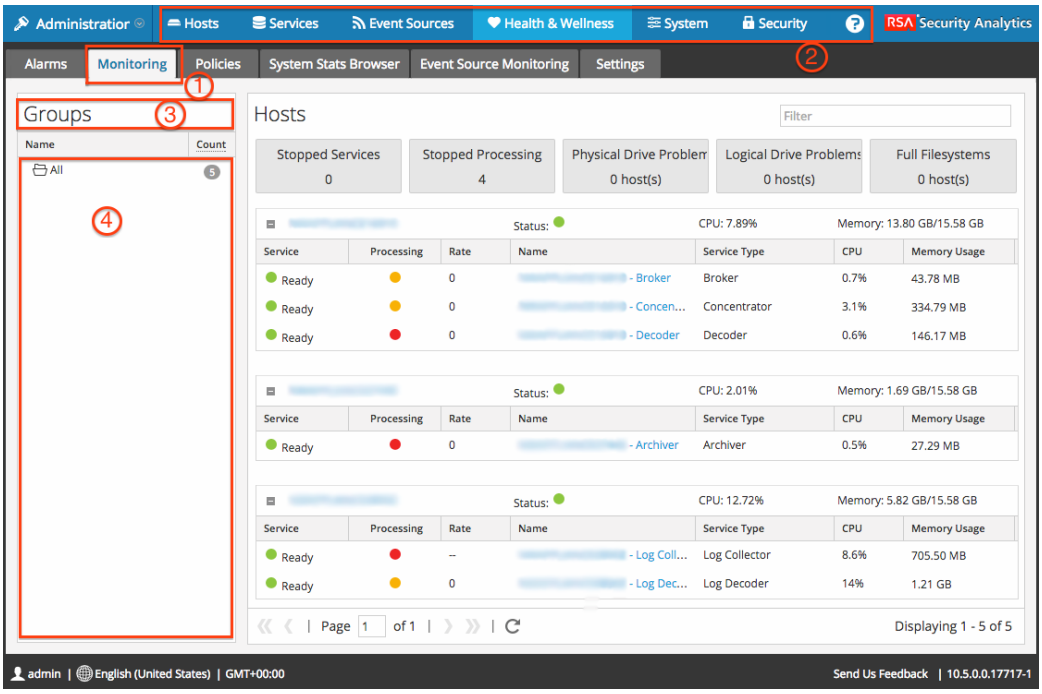
Features

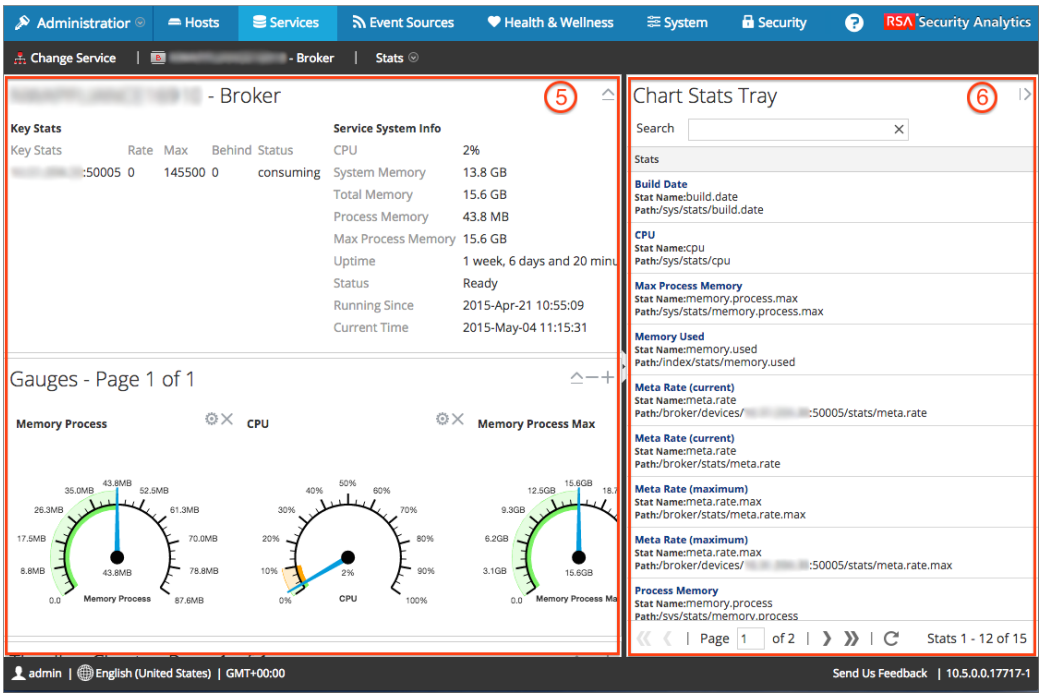
Each view has different features. Any combination of these features is possible in a view:

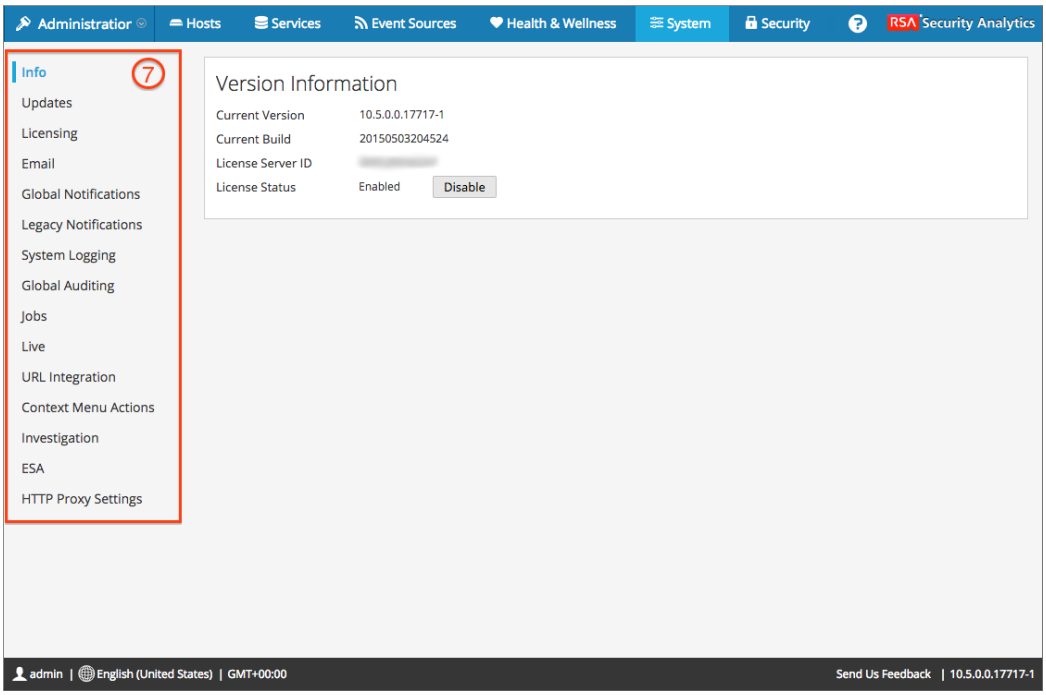
- Toolbars
- Sections
- Panels: there are two different types of specialized panels, options panel and node tree
- Tabs
- Breadcrumbs

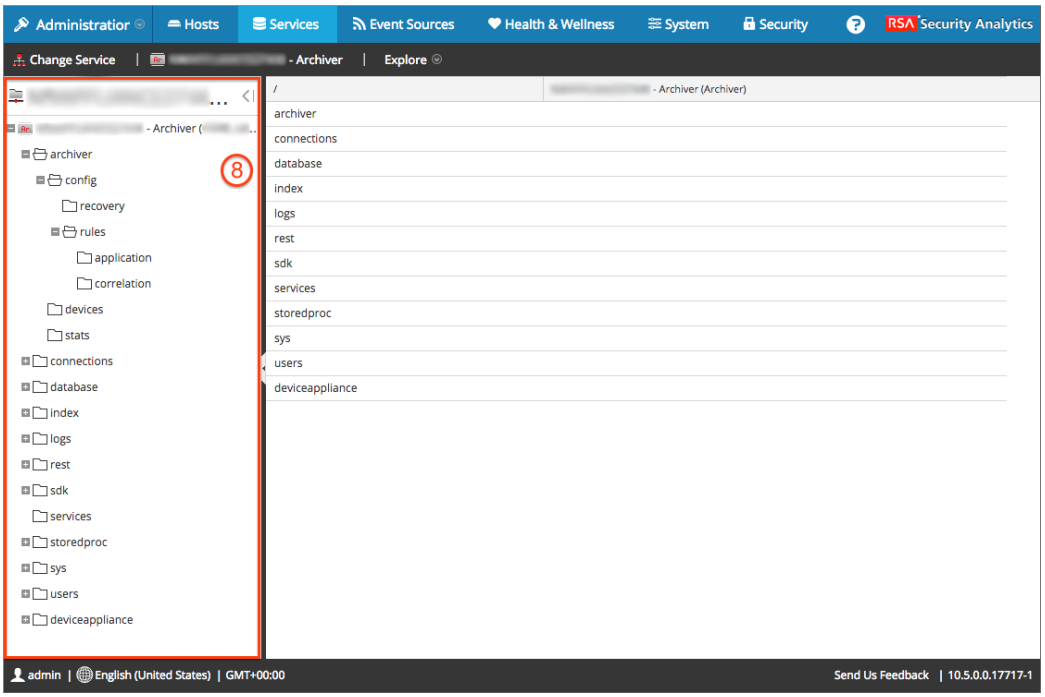
- Grids or tables
- Context menus

The general parts of a view are labeled in the figures below.









The following table provides descriptions of the features labeled above.

Key	Feature	Description
1	tabs	Organize the features of a panel into easily viewed and accessible groups so that you don't have to scroll down the page to view everything. If a panel has many options, the tabs make it easier to navigate to the right group of options in a panel.
2	toolbar	A toolbar may apply to the entire view, to a section, or to a panel.
3,4	sections (top to bottom)	Within a panel, some dashboards have sections that organize information from top to bottom; for example, the **Service Info** view has two sections in the **Service** panel, the **Service** section at the top and the **Session Information** section at the bottom. Sometimes you may need to scroll down to view a section near the bottom of the panel.
5,6	panels (left to right)	Within a view, most dashboards have panels that organize information from left to right; for example, the **Service Stats** view has two panels, the main panel on the left and the **Chart Stats Tray** panel on the right. The **Chart Stats Tray** is not the main focus, so it is collapsible to allow more space in the main panel.
7	options panel	The options panel is a panel that lists options available in a view. Frequently, the options panel doesn't have a title. A list of choices without a header are called options.
8	node tree	A node tree is a list of nodes with expandable and collapsible folders.

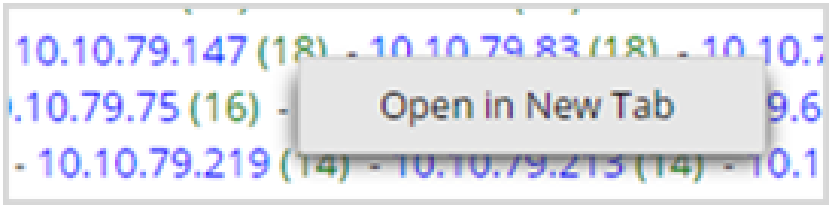
Breadcrumbs

Breadcrumbs display the options selected to reach this view. Click on a crumb to go back to the view or menu. In some modules breadcrumbs have additional functions. For example, in Investigation a breadcrumb represents a sequence of queries used to reach the current drill point and you can edit the query directly from the breadcrumb.

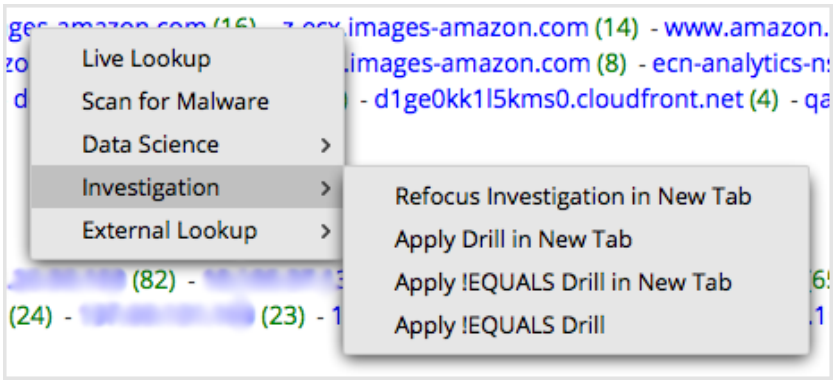
Context Menus

Context menus offer options that pertain specifically to the current context. In certain views, hovering over an item and right-clicking the mouse displays the options that can apply to that item. Throughout the Security Analytics documentation, context menus are discussed in the pertinent modules and views.

A good example of a context menu is shown in the **Navigation** view. When you right-click a count for a meta value (the green number in the parentheses), the menu offers one option: to open the drill in a new tab.



When you right-click on the meta value (blue text), a different context menu is displayed. In this context, there are options to scan for malware, look up the value in Investigation and to display the same drill in a new tab, apply the reverse of this drill (!EQUALS) in the same tab, or apply the reverse of this drill in a new tab.



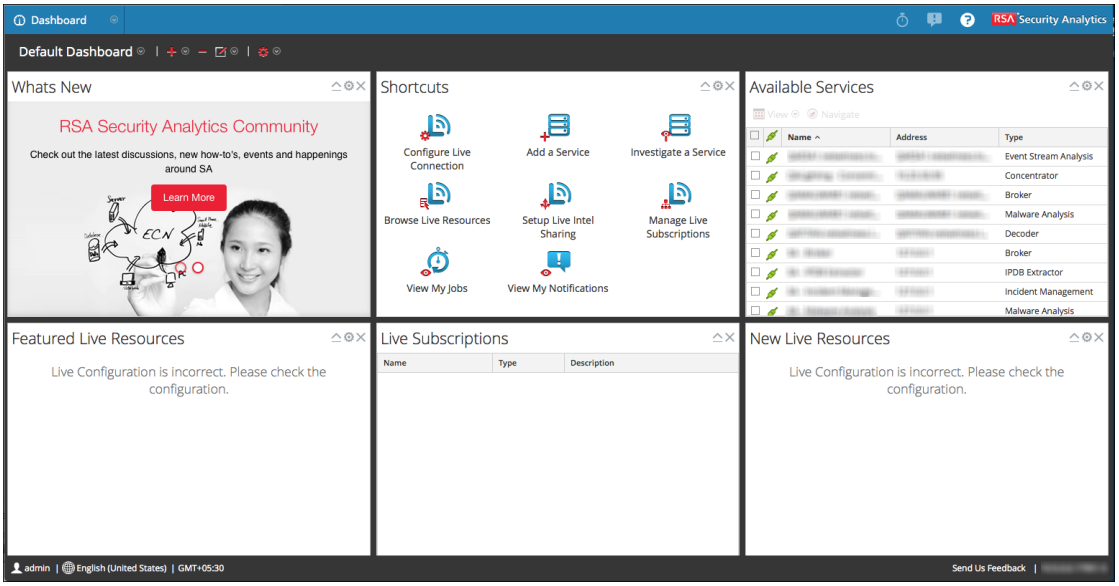
Dashboards

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

By default, the Security Analytics Dashboard is displayed when you log into Security Analytics, and it is populated with a few useful dashlets to get you started with your own customizations. The dashlets for all Security Analytics modules are available to add to the default Security Analytics dashboard or a custom Security Analytics dashboard.

To display the **Security Analytics** dashboard, do one of the following:

- Log on to Security Analytics, and the application opens to the Security Analytics dashboard.
- In the **Security Analytics** menu, select **Dashboard**.



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 dashlets, adding dashlets, moving dashlets, maximizing dashlets, and deleting dashlets.

- After modifying the default dashboard, you can restore the default dashboard to its original layout.
- The default dashboard cannot be deleted.

Note: From 10.6.3 onwards, the Admin Service Monitor dashlet is not available.

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.

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 Dashboards Selection List
- Zero or more dashlets

Out-Of-The-Box Dashboards

Out-Of-The-Box dashboards are dashboards that will be available to the user on upgrade to 10.6.3. By default, these dashboards are disabled on Security Analyticsinstallation. For more information on each Out-Of-The-Box dashboards, see the OOTB Dashboards PDF.

Dashboard Title

The dashboard title reflects the current module; for example, Dashboard.

Dashboard Toolbar

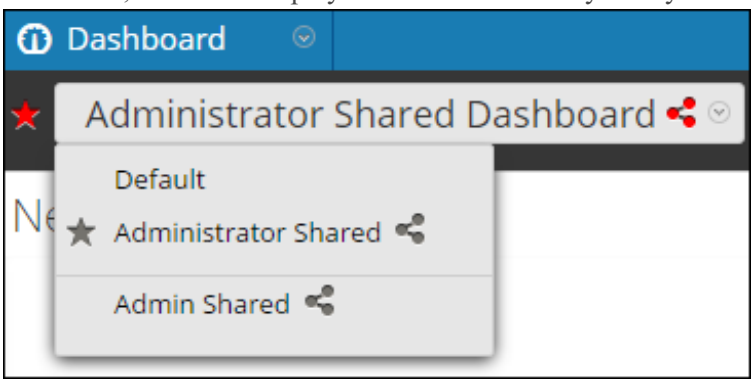
The dashboard toolbar is available next to the current dashboard title. The dashboard toolbar allows various operations on dashboards and dashlets.

Option	Description
Favorite	Sets the selected dashboard as Favorite.
Add Dashlet	Displays the Add a Dashlet dialog, where you add a dashlet to the current dashboard.
Remove Dashboard	Deletes a custom dashboard. The default dashboard cannot be deleted.
Change Dashboard Layout	Displays the Change Dashboard Layout dialog, where you change the layout of the dashboard to one of five options.
Create New Dashboard	Displays the Create a Dashboard dialog, where you define a custom dashboard.
Rename Dashboard	Displays the Rename Dashboard dialog, where you change the dashboard title.
Restore Default Dashboard	Restores the default dashboard to its original appearance, with the default dashlets in their original positions.
Copy Dashboard	Creates a copy of a dashboard which can be shared with other roles to be modified.
Export Dashboard	Creates a .cfg file containing the structure of the current dashboard.
Import Dashboard	Adds a dashboard based on the previously exported .cfg file.
Share Dashboard	Shares a dashboard with other roles for viewing.

Note: The delete, export, and share options are not available for OOTB Dashboards.

Dashboard Selection List

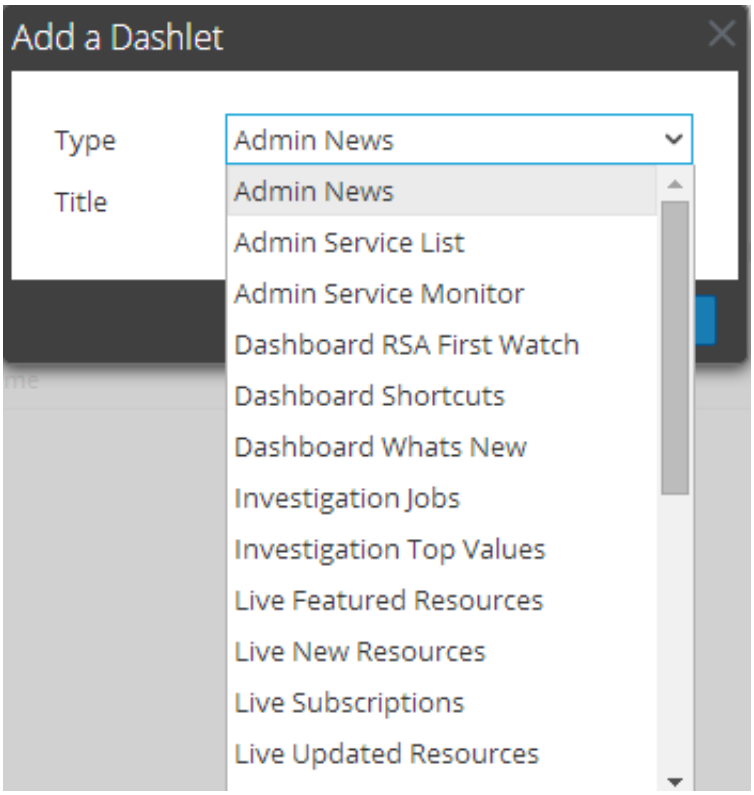
You can access custom dashboards on the Dashboard selection list. When you select a custom dashboard, its title is displayed below the Security Analytics toolbar.



Dashlets

Security Analytics uses dashlets to display focused subsets of system information, services, jobs, resources, subscriptions, rules, Incident Queue activity, Incident Analysts activity, and other information.

Security Analytics modules can display only those dashlets presented in the Add a Dashlet dialog. The main dashboard offers all Security Analytics dashlets. This is an example of currently available dashlets.

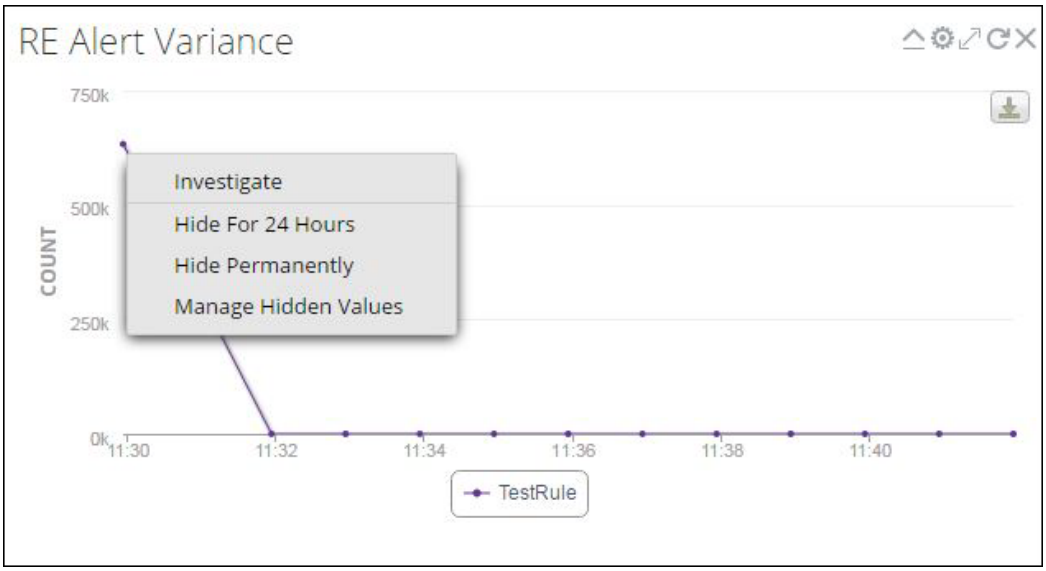


Controls for a dashlet are in the title bar. All dashlets use a common set of controls, and only those that apply to the particular dashlet appear in the title bar.

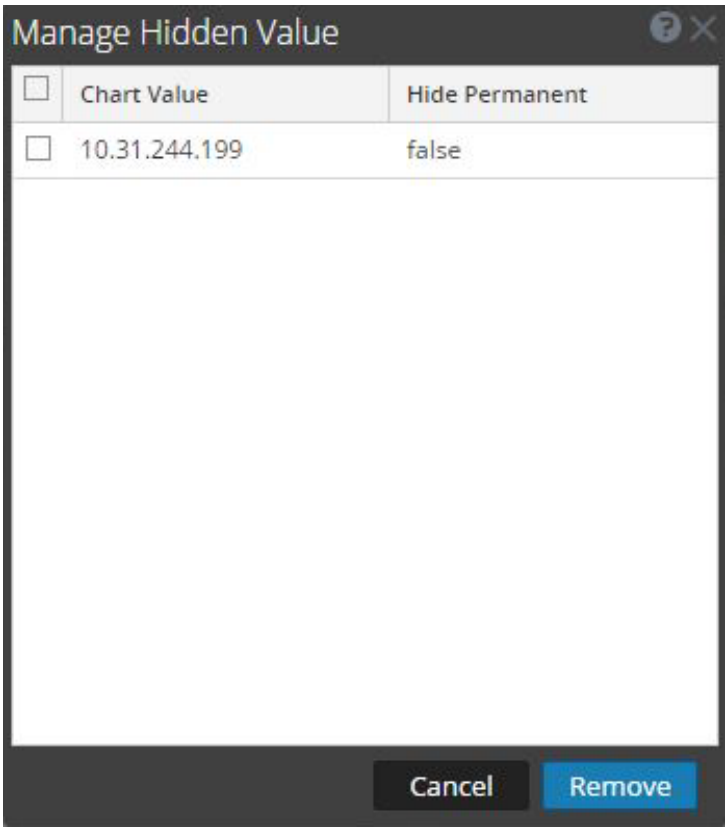
Icon	Name	Description
	Collapse vertically	Collapses the dashlet vertically so that only the title is visible.
	Expand vertically	Expands the dashlet to its original size.
	Page forward	In dashlets with more than one page, moves to the next page.
	Page back	In dashlets with more than one page, moves to the previous page.
	Last Page	In dashlets with more than one page, moves to the last page.
	First Page	In dashlets with more than one page, moves to the first page.
	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.

The following options have been added to 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 data for a selected value for the next 24 hours. After 24 hours, the data will automatically be displayed on the dashlet, if the value is on the top.
- Hide Permanently: This option allows you to hide the data for a selected value permanently.



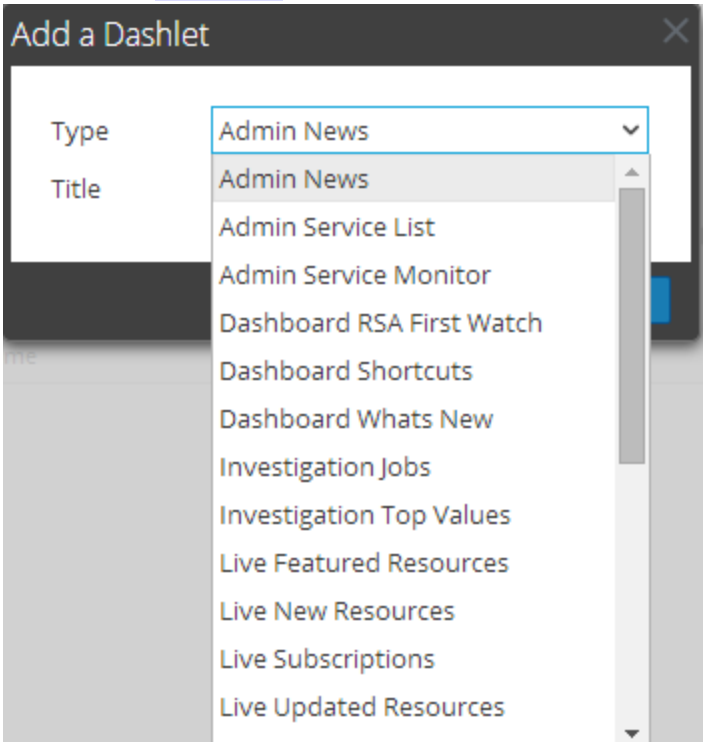
- Manage Hidden Values: This option displays a list of all the hidden values. You can select the checkbox for a value and click **Remove** to unhide the data.



Note: These options are available for Default, Custom, and OOTB Dashboards but it is not available for Shared Dashboards. However, when you edit a value in an OOTB Dashboard it is an user-specific change. The changes made to an OOTB Dashboard will be applicable only to your dashlet and cannot be viewed by other users who use the same OOTB Dashboard. For example, if you hide a value in an Overview Dashboard, the change will be applicable only to your dashlet. If an another user views the same Overview Dashboard, the value will still be displayed.

Dashlets

Dashlets for all Security Analytics modules are available to add in the default Security Analytics dashboard or a custom Security Analytics dashboard. All dashlets have a common set of controls described in Dashboards. This is an example of some currently available dashlets.



Some dashlets have additional configuration parameters and controls, for example the Reports Realtime Chart, Malware and Top Listing of Highly Suspicious Malware dashlets. For more information on these additional controls, read the topic that pertains specifically to that dashlet.

Getting Started with Security Analytics: Terminology

A

Term	Description
Administration module	The Administration module is the user interface for administering and monitoring appliances, devices, and services. When configured, appliances, devices, and services are available to other Security Analytics modules.
Alerts	The Security Analytics Alerts module is the user interface for automated alerting functions.
Anonymised data	"Data are anonymised if all identifying elements have been eliminated from a set of personal data. No element may be left in the information which could, by exercising reasonable effort, serve to re-identify the person(s) concerned. Where data have been successfully anonymised, they are no longer personal data." (Source - EU_DP_LAW_HANDBOOK) This term is defined as part of the Security Analytics data privacy solution.
anonymization	The Privacy Technology Focus Group defines anonymization as a technology that converts clear text data into a nonhuman readable and irreversible form, including but not limited to one-way hashes and encryption techniques in which the decryption key has been discarded. This term is defined as part of the Security Analytics data privacy solution.
Archiver	The RSA Archiver is an appliance that enables long-term log archiving by indexing and compressing log data and sending it to archiving storage.

B

Term	Description

Term	Description
Broker	The RSA Broker is an appliance and a service in the Security Analytics network. Brokers aggregate data captured by configured Concentrators, and Concentrators aggregate data from Decoders. Therefore, a Broker bridges the multiple real-time data stores held in the various Decoder/Concentrator pairs throughout the infra-structure.

C

Term	Description
capacity	Security Analytics 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.
collections	Collections are log retention sets for storing log data. For each collection, you can specify how much of the total storage space to use and how many days to retain the logs in the collection. You configure collections in Archiver.
Concentrator	The RSA Concentrator is an appliance and service in the Security Analytics network. Concentrators index 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.
Core Data-base	This refers to the combination of the Packet, Meta, Session, and Index data.
Core ser-vices	In Security Analytics, the Core services ingest and parse data, generate meta data, and aggregate generated meta data with the raw data. The Core services are Decoder, Log Decoder, Concentrator, and Broker.

D

Term	Description
dashboard	The Security Analytics dashboard is the user interface displayed in a browser when logged on to Security Analytics. It can also be referred to as the dashboard in the generic sense. For example: You can create custom dashboards in the Security Analytics dashboard. In the specific sense "Security Analytics dashboard" replaces "Unified Dashboard".
Decoder	The RSA Decoder is an appliance and service in the Security Analytics network. In the Security Analytics network, packet data is collected using an appliance called Decoder, while the Log Decoder collects log events. The Decoder captures, parses, and reconstructs all network traffic from Layers 2 - 7, or log and event data from hundreds of devices.
downstream system and components	As opposed to core components, downstream systems use data stored on Core services for analytics, therefore, the operations of downstream services are dependent on Security Analytics Core services. The downstream systems are Archiver, Warehouse, ESA, Malware Analysis, Investigation, and Reporting.
drill point	A set of data that an analyst has brought into focus using queries and filters in the Investigation view. In effect, the analyst drills into the captured data to find interesting data that may harbor harmful files or code.

E

Term	Description
Event Stream Analysis (ESA)	The RSA Event Stream Analysis (ESA) appliance 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 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.

Term	Description
EVP	Events per second is a measure of the processing capacity for an RSA host that is consuming data.

F

Term	Description
Forensics implementation	In a forensics implementation, the base Security Analytics configuration requires these components: Decoder, Concentrator, Broker, ESA, and Malware Analysis. An optional component is the Incident Management service, which resides on the ESA system and is used to prioritize alerts.
FirstWatch	RSA FirstWatch is a research and analysis organization focused on emerging, sophisticated threats around the globe. Tracking over 5 million IPs and domains and dozens of unique threat sources, RSA FirstWatch delivers situational awareness and threat intelligence from across RSA's research and incident response community.

G

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

H

Term	Description
hashing	An obfuscation method used to protect sensitive data.

Term	Description
host	Physical equipment or virtual machine, designated by a Fully Qualified Domain Name (FQDN) or IP address, on which any Security Analytics service is installed [that is the Security Analytics server, appliance service, Archiver service, Broker service, Concentrator service, Broker service, Decoder service (Packets and Logs), Hybrid, Malware Analysis service, Event Stream Analysis service, Log Collector service, Security Analytics Warehouse service, Workbench service, Reporting Engine service, and IPDB Extractor service].

I

Term	Description
Term	Description
Identifiability	"An individual is identified in this information; or if an individual, while not identified, is described in this information in a way which makes it possible to find out who the data subject is by conducting further research." (Source - EU_DP_LAW_HANDBOOK) This term is used when discussing the Security Analytics data privacy solution.
Incident Management service	The Incident Management service resides on the ESA system and is used to prioritize alerts.
Incidents module	The Incidents module provides the Incident Management function in Security Analytics. The incident management function is an easy way to track the incident response process.
Index	The index is a collection of files that provides a way to look up Session IDs using meta values.
Investigation module	The Investigation module is the Security Analytics user interface that allows visualization and reconstruction of packets and logs captured by Security Analytics appliances.

J

Term	Description
Job system	The Security Analytics jobs system lets you begin a long-running task and continue using other parts of Security Analytics 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 success or failure. While you are working in Security Analytics, you can open a quick view of your jobs from the toolbar.

L

Term	Description
Live module	The Live module is the Security Analytics user interface to access and manage resources available to customers through the Live Content Management System.
Log Decoder	A Log Decoder is a type of Decoder that collects logs rather than packets. It can collect four different log types - Syslog, ODBC, Windows eventing, and flat files.

M

Term	Description
Malware Analysis	Malware Analysis is an appliance and a co-located service in Security Analytics. The service is used for automated malware analysis and is accessible through the Investigation module.
Message Digest	Uses a one-way hash function to turn an arbitrary number of bytes into a fixed-length byte sequence. This is used as part of a data privacy solution.
meta DB	The meta database contains items of information that are extracted by a Decoder or Log Decoder from the raw data stream. Parsers, rules, or feeds can generate meta items.
meta ID	A number used to uniquely identify a meta item in the meta database.

Term	Description
meta data or meta items	A Decoder ingests and parses raw data, creating meta items (meta data) in the process.
meta key	A name used to classify the type of each meta item. Common meta keys include ip.src, time, or service.
meta value	Each meta item contains a value. The value is what each parser, feed, or rule generates.
metered licensing	Metered licensing is a Security Analytics licensing method based on a throughput per day of logs (SIEM) or network packets (Network Monitoring and Network Malware), combined with the separate purchase of the hardware needed to deploy the system and meet customers' retention requirements.

N

Term	Description
NetWitness or NextGen device	An RSA Broker, Concentrator, Decoder, Log Decoder, or Log Collector. If you see the term NextGen device, or NetWitness device change it to Core device.

O

Term	Description
Out-of-the-box trial licensing	Security Analytics 10.5 ships with a default Trial out-of-the-box license that enables customers to use the product with full functionality for 90 days. The 90-day time period begins when the Security Analytics user interface is configured and used for the first time.

Term	Description
Out-of-Compliance banners	A red banner is displayed during log on if your license is expired or you have exceeded your allotted usage. You may also see a red banner if your license has internal errors. A red banner cannot be dismissed. A yellow banner is displayed during system log on if your license is approaching expiration or you are nearing your allotted usage. You can dismiss the yellow banner by clicking the Dismiss button.

P

Term	Description
packet ID	A number used to uniquely identify a packet or log in a packet database.
packet DB	The packet database contains the raw, captured data. On a Decoder, the packet database contains packets as captured from the network. Log Decoders use the packet database to store raw logs. The raw data stored in the packet database is accessible by a Packet ID, however, this ID is typically never visible to the end user.
Personal data	"Under EU law, personal data are defined as information relating to an identified or identifiable natural person, that is, information about a person whose identity is either manifestly clear or can at least be established by obtaining additional information." (Source - EU_DP_LAW_HANDBOOK)

R

Term	Description
RSA Analytics Warehouse	A Hadoop-based distributed computing system, which collects, manages, and enables analytics and reporting on longer-term sets of security data, for example, months or years. The Warehouse can be made up of three or more nodes depending on the organization's analytic, archiving, and resiliency requirements. It requires a service called Warehouse Connector to collect meta and events from Decoder and Log Decoder and writes them in Avro format into a Hadoop-based distributed computing system.

Term	Description
Reports module	The Reports module is the Security Analytics user interface for automated reporting functions.
Roles	In Security Analytics, roles determine what users can do. A role has permissions assigned to it and you must assign a role to each user. The user then has permission to do what the role allows.

S

Term	Description
Security Analytics Core (formerly NextGen)	The following products are part of the Security Analytics Core suite: Decoder, Log Decoder, Concentrator, Broker, Archiver, Workbench.
Security Analytics Server	The web server for reporting, investigation, administration, and other aspects of the analysts interface. Also enables reporting on data held in the Warehouse.
Sensitive data	Regulatory mandates in some locations, for example the European Union (EU), require that information systems provide a means of protecting data when operating on sensitive data. Any data that could directly or indirectly depict "Who did what when?" may be considered personally identifiable or sensitive data.
Service	A service runs on a host and performs a unique function, such as collecting logs or archiving data. Security Analytics services include Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, Incident Management, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, and Workbench.
Service-based licensing	This is a per-service permanent Security Analytics license that has no expiration date. Support for service-based licensing is applicable for all appliances that require a license.

Term	Description
session	On a packet Decoder, a session represents a single, logical, network stream. For example, a TCP/IP connection is one session. On a Log Decoder, each log event is one session. Each session contains references to all the Packet IDs and Meta IDs that refer to the session.
session ID	A number used to uniquely identify a session in the Session DB.
session DB	The session database contains information that ties the packet and meta items together into sessions.
SIEM implementation	In a security information and event management (SIEM) implementation, the base Security Analytics configuration requires these components: Log Decoder, Concentrator, Broker, Event Stream Analysis (ESA), and the Security Analytics server.
Subscription licensing	Subscription licenses for Security Analytics are offered for a specific time period that ranges from 12 to 36 months. Once licensed, subscription licenses are non-cancellable and non-downgradeable.

T

Term	Description
Transient data	In Security Analytics, transient data is not stored on disk. When a meta key is marked as transient in the custom index file or the Services Config view where parsers for the service are configured, the Decoder, Log Decoder does not save the meta key to disk, but holds it in memory where it can be analyzed until overwritten.

V

Term	Description
Virtual host	(Formally virtual appliance) Virtual machine, designated by a Fully Qualified Domain Name (FQDN)) or IP address, on which any Security Analytics service runs (that is the appliance service, Archiver service, Broker service, Concentrator service, Broker service, Decoder service (Packets and Logs), Hybrid, Malware Analysis service, Event Stream Analysis service, Log Collector service, Security Analytics Warehouse service, Workbench service, Reporting Engine service, and IPDB Extractor service. A virtual instance of a Security Analytics appliance.

W

Term	Description
Warehouse Connector	Warehouse Connector collects meta and events from Decoders and writes them in Avro format into a Hadoop-based distributed computing system. You can set up Warehouse Connector as a service on existing Log Decoders or Decoders or it can be run as a virtual appliance in your virtual environment.
Windows eventing	Windows eventing pertains to Log Decoders, and refers to the Windows 2008 collection methodology and flat files can be obtained via SFTP.

Getting Started with Security Analytics: Procedures

In Security Analytics, users must open a browser and log on. To make the most of Security Analytics, you need to know how to manage jobs and notifications, configure dashboards and grids, customize application settings such as language and time zone, and change your password.

These procedures are intended for all users learning to work in Security Analytics.

Accessing Security Analytics

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

Note: If you are logging on to Security Analytics from an Internet Explorer 10 browser window, the following error may be displayed:
`The page can't be displayed.` You need to enable the TLS 1.1 protocol in your browser as follows:
Navigate to **Internet options > Advanced > Settings > Security**. In addition to your other protocols, ensure that the TLS 1.1 protocol is enabled. Click **Apply**. Reload the page.

When you attempt to log in to Security Analytics, your account can be in one of the following states:

- **Valid:** You can successfully log on to Security Analytics.
- **Locked out:** You are unable to log on because there were too many attempts to log in to your account with bad credentials. This is temporary. Contact your Administrator for assistance.
- **Expired:** You can authenticate to Security Analytics, but you must change your password before accessing Security Analytics.

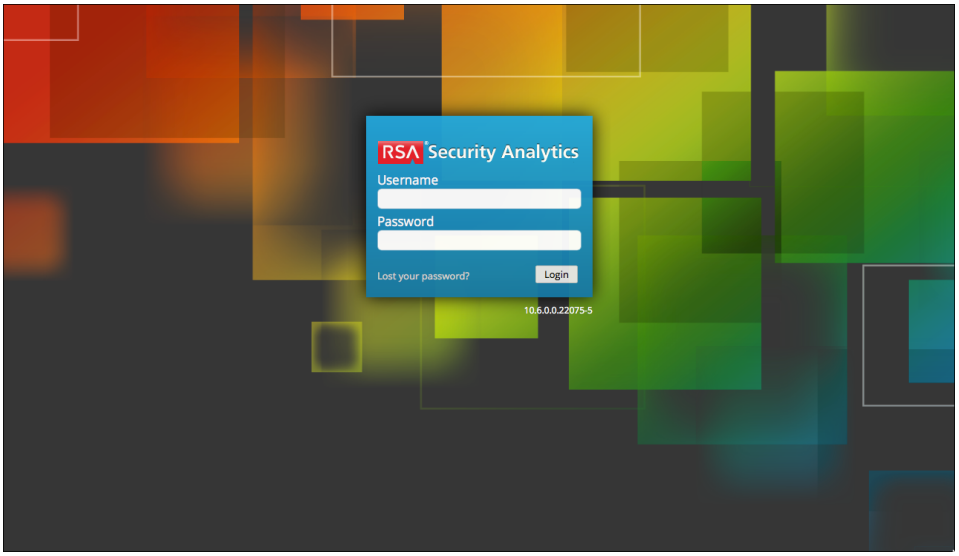
To access Security Analytics:

1. Use a Security Analytics 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 Security Analytics server.

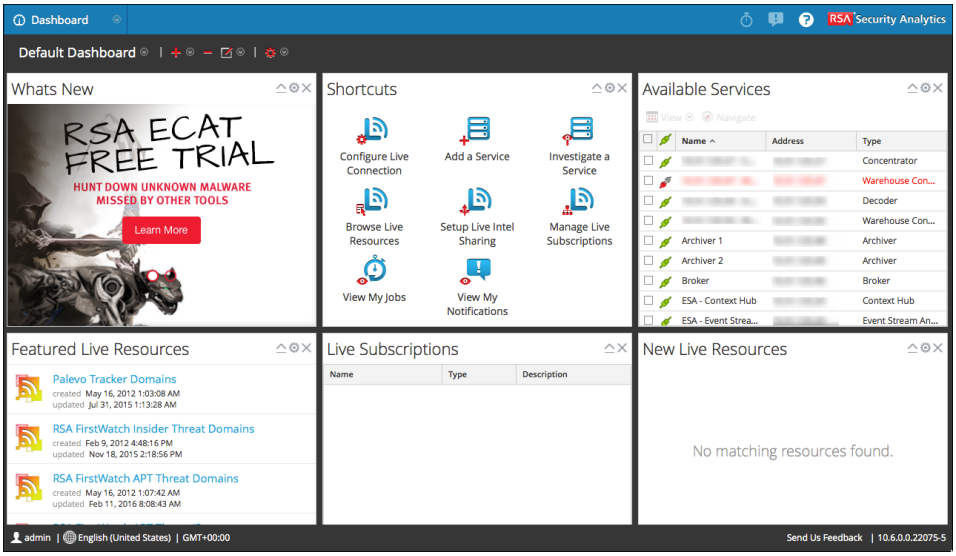
   The Security Analytics login screen is displayed.



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

   If your Login is successful, you will see an initial view based on your user profile preferences.

The following figure shows an example of the Security Analytics default dashboard.

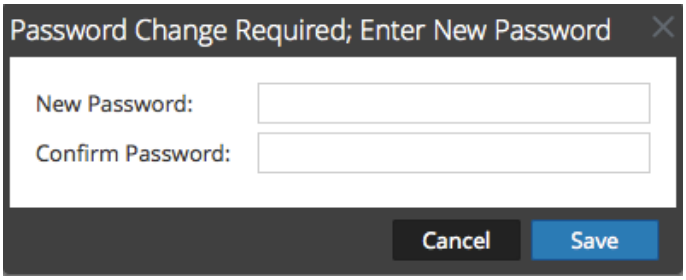


If you are locked out:

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 your account is expired:

1. In the dialog box, type a new password, confirm it, and click **Save**.

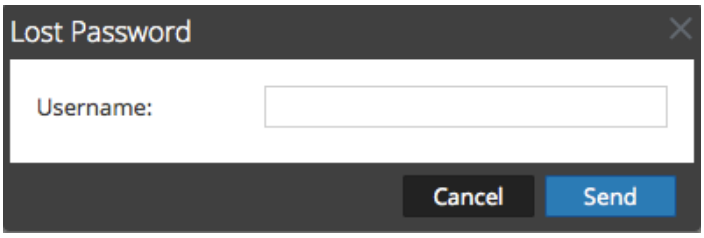


2. Click **OK** to confirm that your password was successfully changed.

   You have a maximum of 5 minutes to enter your new password. Your session could time out sooner depending on the session and idle time security settings set by your Administrator. If your session times out, log in again with your old password and then change your password.

If you forgot your password:

1. On the Security Analytics login screen, click the **Lost Your Password?** link.
2. In the **Lost Password** dialog, type your username and click **Send**.



You should receive an email with instructions. If you do not receive an email, contact your Administrator to add an email address to your account.

If you do not have the appropriate access to Security Analytics:

If you are able to log in successfully to Security Analytics, 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.

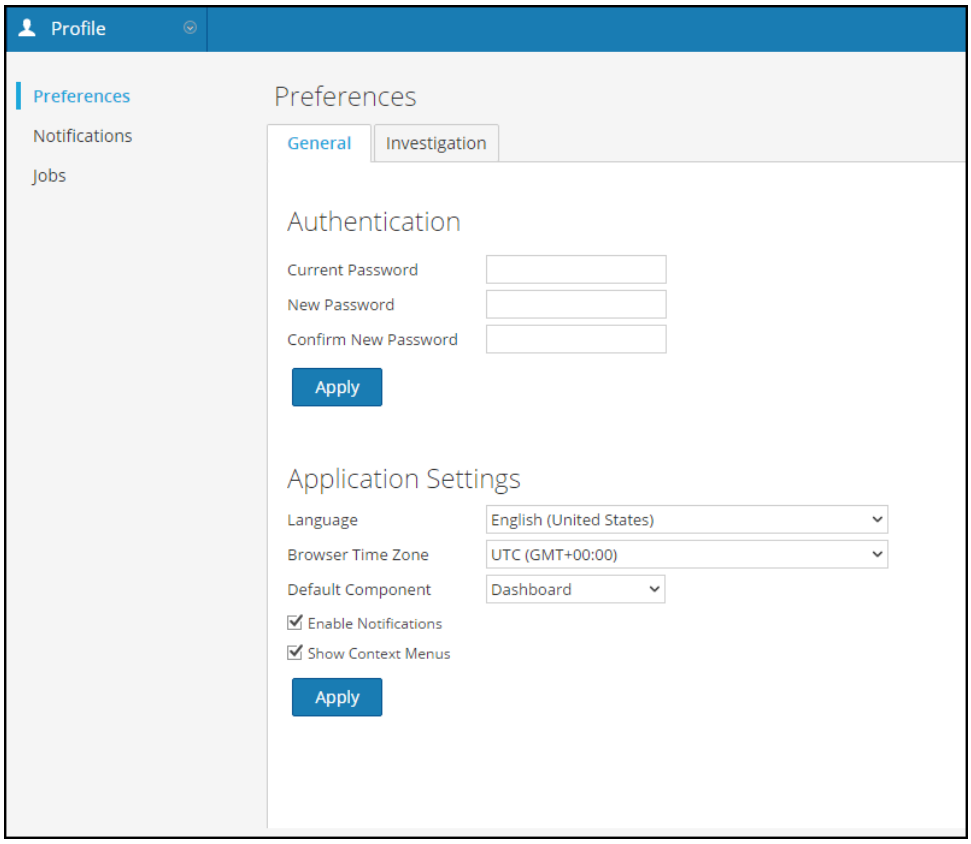
Changing Your Password

Users can change the password that they use for Security Analytics authentication in the Profile View > Preferences panel. The password of the user is updated on Security Analytics Core services, unless the user is the admin user. The password of the admin user does not propagate to Core services.

Note: For Core services, this applies to untrusted connections only. When a Core service uses a trusted connection, the user does not enter a password so no update is required.

To change your Security Analytics password:

1. In the **Security Analytics** menu, select **Profile.**
2. In the options panel, select **Preferences**.
   The Preferences panel is displayed with the General tab open.



3. In the **Authentication** section, in the **Current Password** field, enter your current password that you used to authenticate Security Analytics.
4. In the **New Password** field, enter the password you want to use for the next login.
5. In the **Confirm Password** field, re-enter the same password to confirm.
6. Click **Apply**.
   You will be logged out from Security Analytics for the changes to take effect. The new password becomes effective form the next time you log on to Security Analytics.

Configuring Application Preferences

User preferences that apply to the Security Analytics application in general are documented in this section. Preferences that apply specifically to Investigation are described in the **Configure Navigate View and Events View** topic in the *Investigation and Malware Analysis Guide*.

You can view and manage different user preferences in the Preferences panel. You can:

- Set the application language
- Set the browser time zone

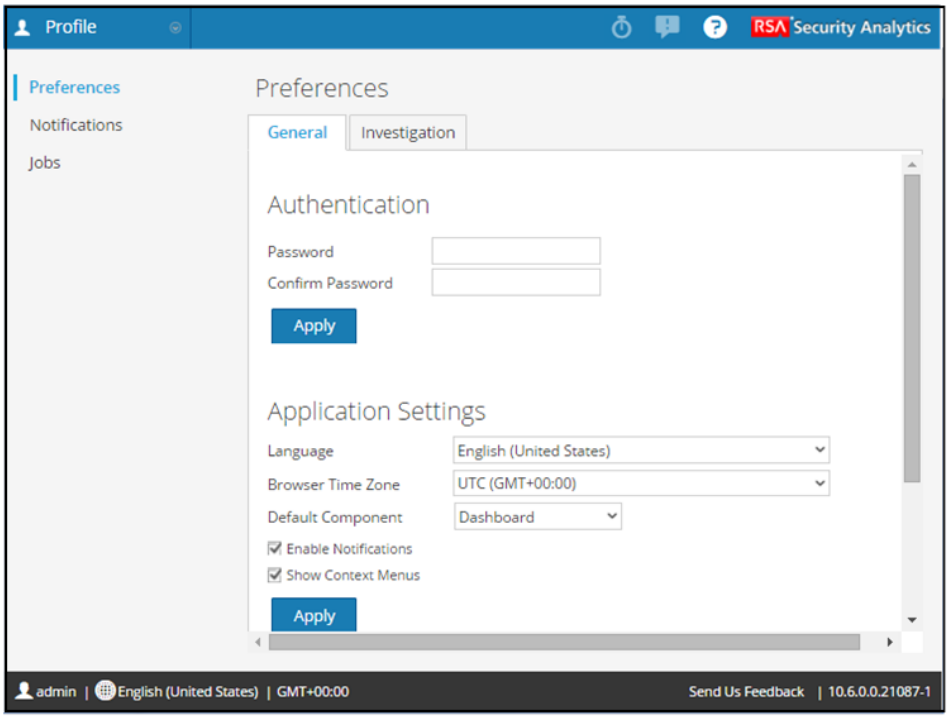
- Set the default component
- Enable notifications
- Enable context menus

These preferences apply to your own profile.

View User Preferences

To view user preferences:

1. In the **Security Analytics** menu, select **Profile.**
2. In the options panel, select **Preferences**.



Set the Language, Browser Time Zone, and Default Component for Security Analytics

The default language for all of the dashboards, dashlets, views, and dialogs that you see is the preferred language that your browser sends. If Security Analytics is not localized to that language, the default language is English (United States). You can change the language to other languages in which Security Analytics has been localized. These settings can be configured in the **Application Settings** section.

To change the language, browser time zone, and default component of Security Analytics:

1. Select a localization in the **Language** drop-down list.
2. Select a time zone in the **Browser Time Zone** drop-down list.
3. Select the component that serves as the opening view when you log on to Security Analytics in the **Default Component** drop-down list.
4. Click **Apply**.
   The selected settings become effective immediately.

Enable or Disable System Notifications for Your User Account

By default, Security Analytics system notifications are enabled when a new user account is created. Each user can change this according to preference.

To enable or disable notifications for your user account:

1. In the **Application Settings** section, click the **Enable Notifications** checkbox.
2. Click **Apply**.
   The new preference becomes effective immediately.

Enable or Disable Context Menus for Your User Account

By default, Security Analytics 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. Each user can change this according to preference.

To enable or disable context menus for your user account:

1. In the **Application Settings** section, click the **Show Context Menus** checkbox.
2. Click **Apply**.
   The new preference becomes effective immediately.

Viewing Help in the Application

These procedures are useful when you are seeking assistance while working in Security Analytics. There are different ways available to get help while using Security Analytics. Options include: Inline help, tooltips, and online help links.

View Inline Help

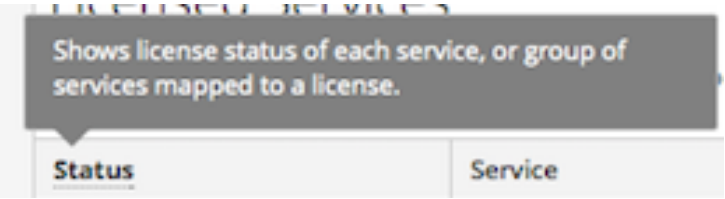
Inline help provides additional information about what to do in sections or fields that you are currently viewing in the Security Analytics user interface. To display inline help, hover over  . Inline help shows a brief description of the element.

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 Security Analytics to the RSA online documentation. This site has a complete documentation set for Security Analytics, and the links take the user 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 Security Analytics toolbar 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 Security Analytics toolbar.

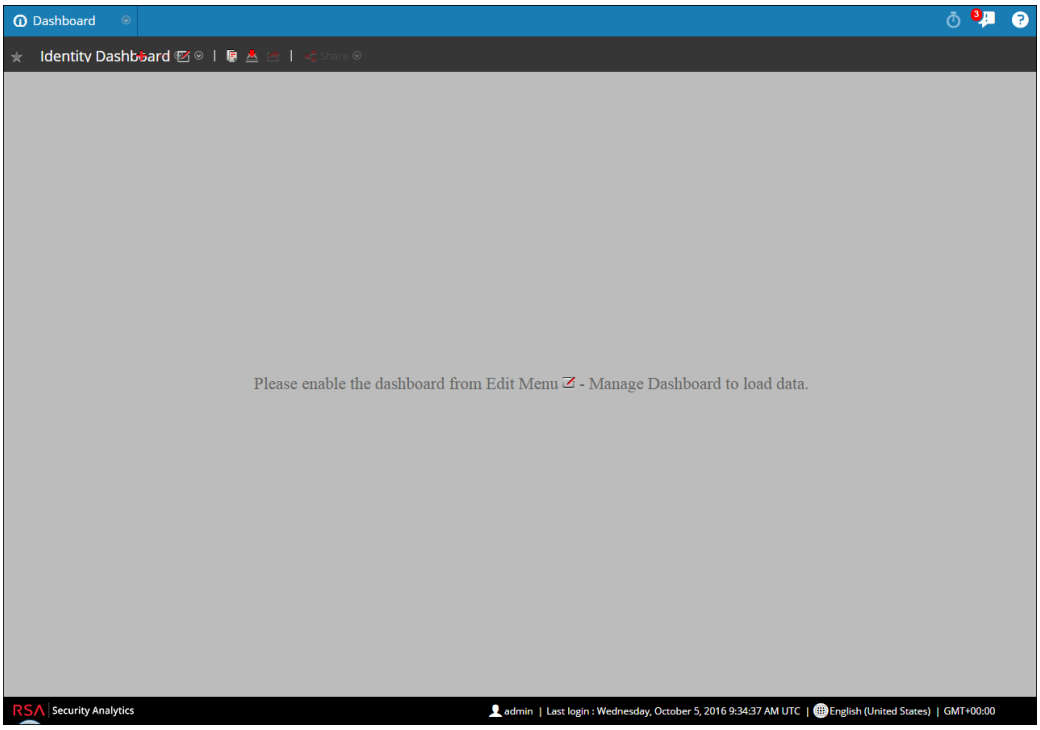
Managing Dashboards

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.

- Enabling a Dashboard
- Disabling a Dashboard

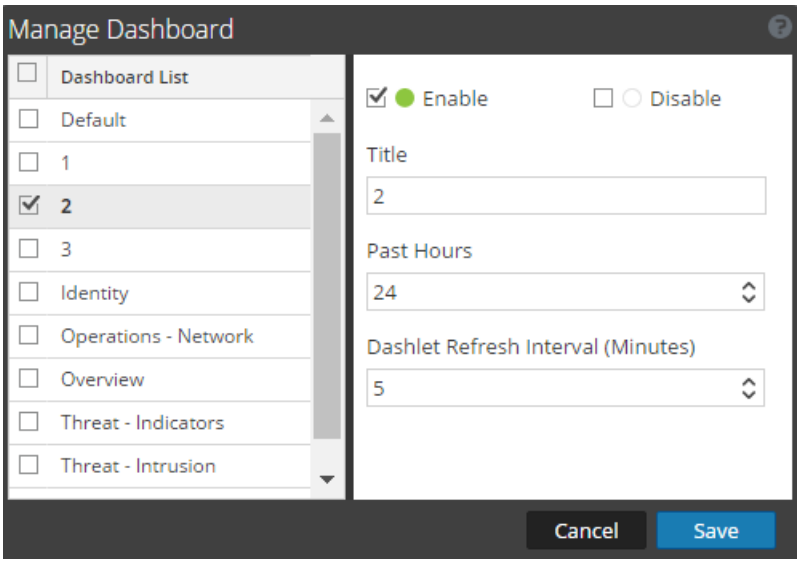
Enabling a Dashboard

When a dashboard 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.
   A Manage Dashboards window is displayed.



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

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

Note: When you select two dashboards at the same time, the fields with the same value will be empty and can be edited.

Name	Description
Dashboard List	Displays a list of the default, Out-Of-The-Box and Custom dashboards.
Enable	Displays if the selected dashlet is enabled.
Disable	Displays if the selected dashlet is disabled.
Title	Displays the titles of the selected dashlet.
Past Hours	Displays the time for which the data is collected.
Dashlet Refresh Intervals (Minutes)	Displays the refresh interval time of a dashlet. For example, if you want the displayed data to refresh every 15 minutes, set this parameter for 15 minutes.

The following table describes the editable fields for different types of Dashboards.

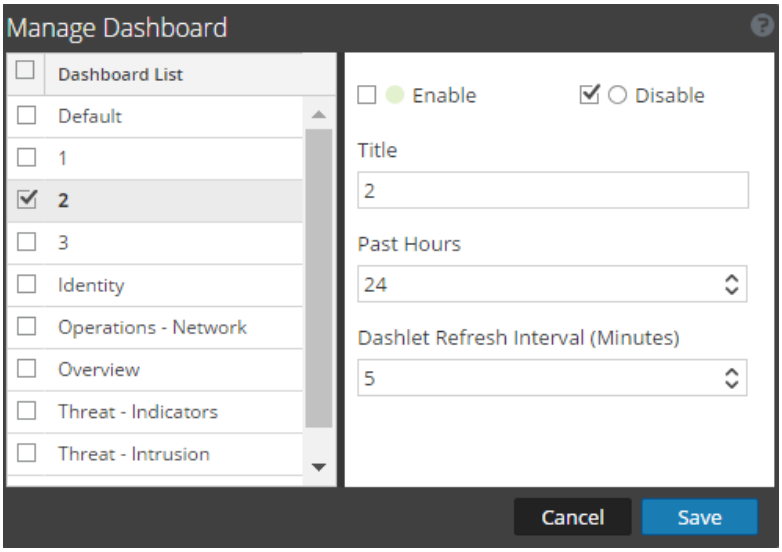
Type Dashboard	Description
OOTB Dashboard	The refresh interval filed is editable.
Custom Dashboard with chart type dashlet	All fields are editable.
Custom Dashboard without chart type dashlet	Only the title field is editable.

Disabling a Dashboard

To disable one or more dashboard(s):

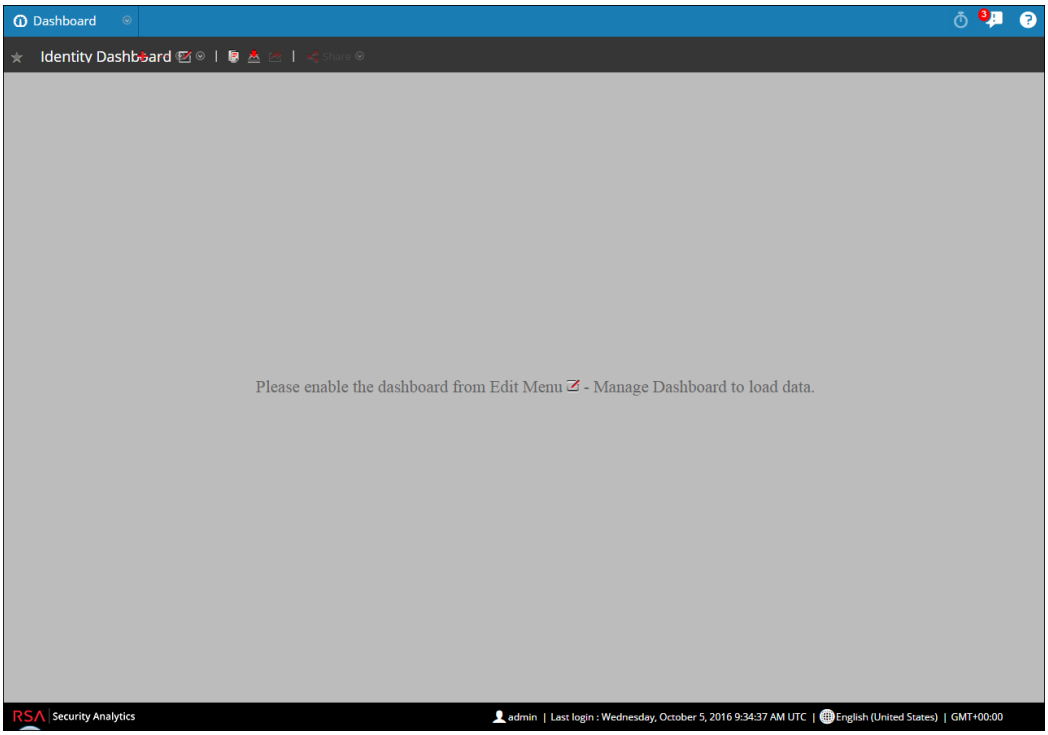
1. Navigate to the dashboard to be disabled.
2. In the dashboard toolbar, click  .

3. Select the **Manage Dashboard** option.
   A Manage Dashboards window is displayed.



4. From the dashboard list, select the Dashboard(s) to be disabled.
5. Click the **Disable** checkbox.
6. Click **Save**.
   A confirmation pop-up is displayed.

If you select a disabled dashboard, a masked screen is displayed.


Dashboard
Identity Dashboard
Please enable the dashboard from Edit Menu - Manage Dashboard to load data.
RSA Security Analytics
admin | Last login : Wednesday, October 5, 2016 9:34:37 AM UTC | English (United States) | GMT+00:00

Configuring Dashboards

As you become more familiar with Security Analytics, there will be types of information that you want to see quickly and easily in the dashboard. You can benefit greatly by configuring your dashboards to display the information that supports your workflow.

Operations that pertain to dashboards include:

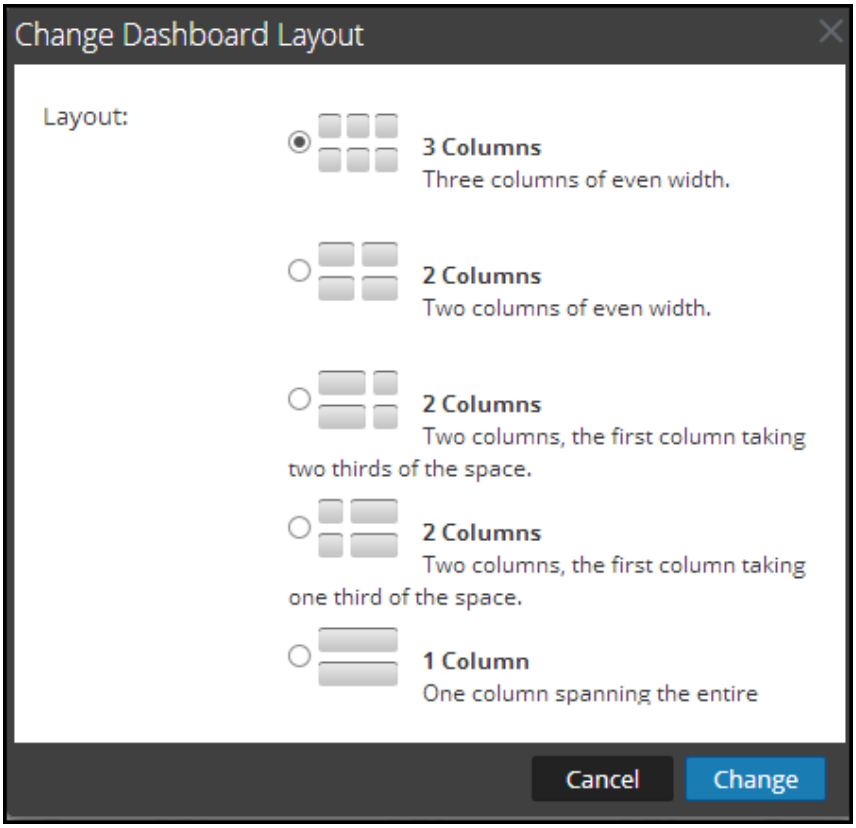
- Arranging the Dashboard Layout
- Adding and Managing Dashlets
- Working with Custom Dashboards
- Working with Out-Of-The-Box Dashboards
- Copying a Dashboard
- Importing and Exporting Dashboards
- Setting a dashboard as Favorite
- Sharing a Dashboard

Arranging the Dashboard Layout

To customize the views in Security Analytics, you can change the layout of the **Security Analytics** dashboard or a custom dashboard.

1. Navigate to any dashboard.
2. In the dashboard toolbar, click the **Edit** drop-down menu ( ) and select **Change Dashboard Layout**.

The Change Dashboard Layout dialog box is displayed.



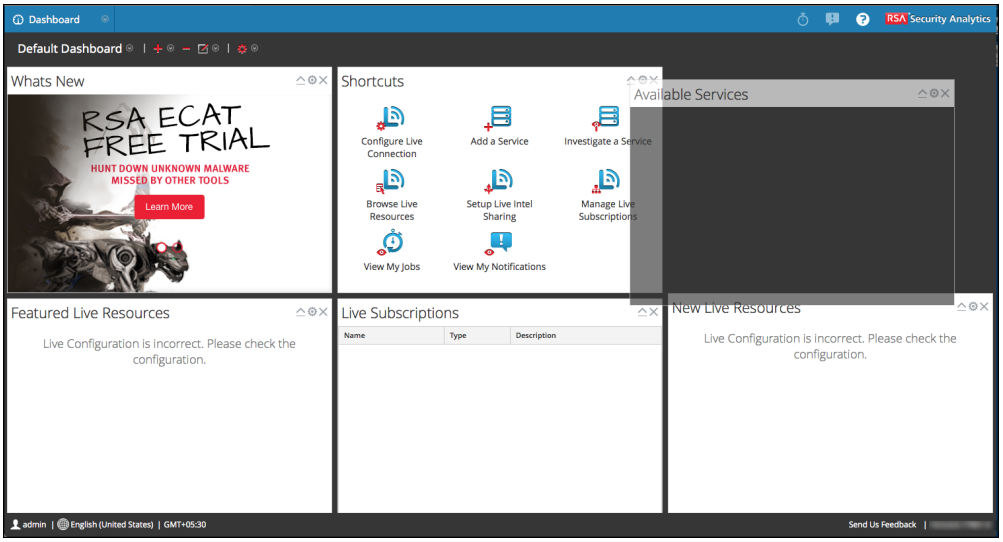
3. Choose a layout for the dashboard and click **Change**.
   The dashboard layout is changed to the selected layout.

Move a Dashlet to a Different Position

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 image below shows the New Live Resources dashlet as it is moved from the bottom

position of column 1 to the top position of column 3.

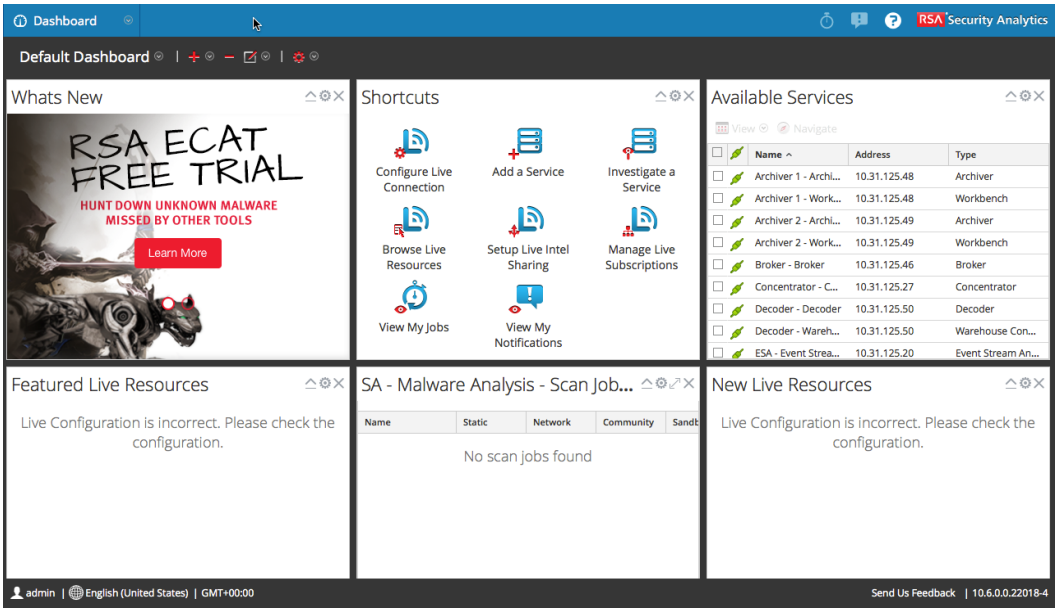


3. Release the mouse button when the dashlet is in the desired location.

   The dashlet that currently occupies that position moves down.

Maximize a Single Dashlet

This topic explains how to open a dashlet on the entire area of the main Security Analytics dashboard with the same dashlet title. For example, the Scan Jobs dashlet from the below figure may be viewed on the entire area of the Security Analytics dashboard. 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.

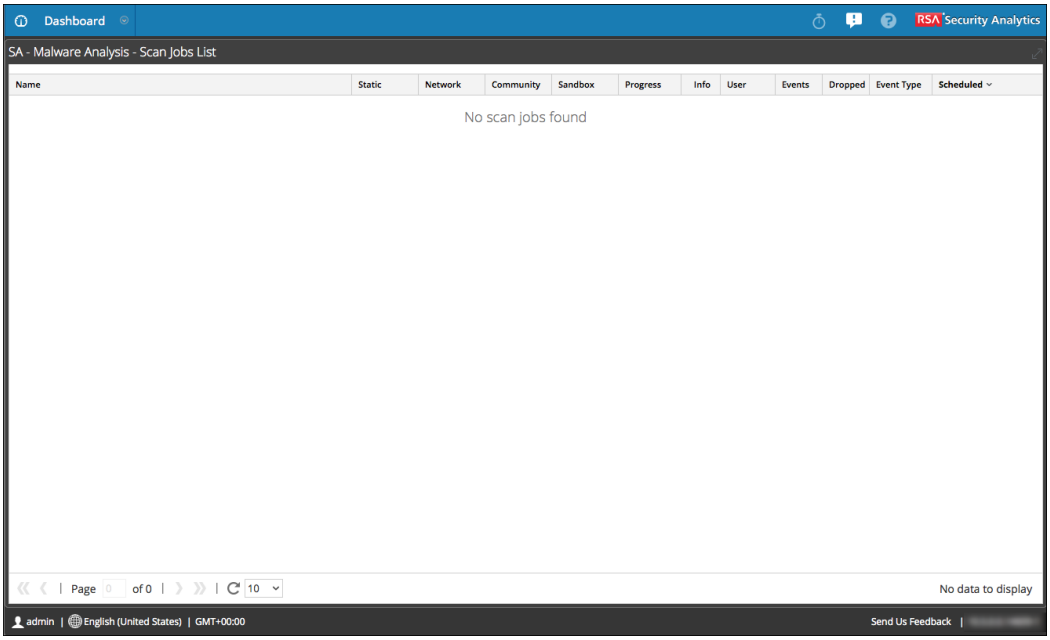


1. To maximize a dashlet, click the maximize control icon ⤢ in the dashlet title bar.

   The dashlet is displayed on full screen.

2. To maximize a dashlet, click the maximize control icon in the dashlet title bar.

   The dashlet is displayed on full screen.



Restore the Default Dashboard

After customizing the default **Security Analytics** dashboard, you can revert to the original layout of dashlets using the **Restore Default Dashboard** option in the **Actions** drop-down ( ). To accomplish this reversion, the dashboard of a module must be displayed.

1. Navigate to the **Security Analytics** dashboard which has been customized.
2. In dashboard toolbar, click the **Actions** drop-down ( ) and select **Restore Default Dashboard**.

   The original layout of the default dashboard is restored.

Adding and Managing Dashlets

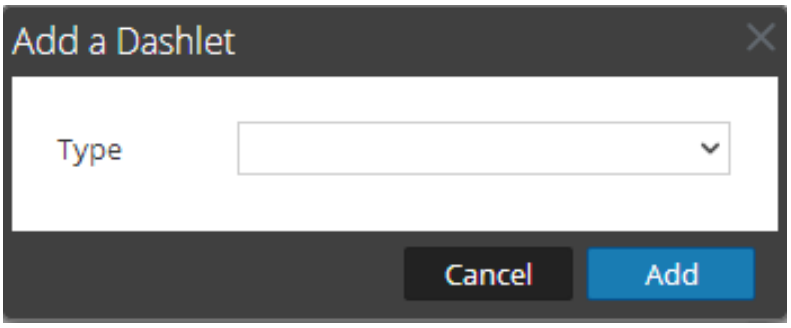
You can add dashlets to the default dashboard or construct a custom dashboard with your own useful set of dashlets to make your workflow more efficient. Some dashlets have configuration options to tailor the appearance or the contents of the dashlet.

Add a Dashlet

To customize the views in Security Analytics, you can add dashlets to the Security Analytics dashboard or a custom dashboard. The Security Analytics dashboard, as the name suggests, offers all Security Analytics dashlets. The Add a Dashlet dialog provides a way to define the name and configurable parameters for a new dashlet.

1. To add a dashlet, navigate to any dashboard.
2. In the dashboard toolbar, click and select **Add Dashlet** from the drop-down menu.

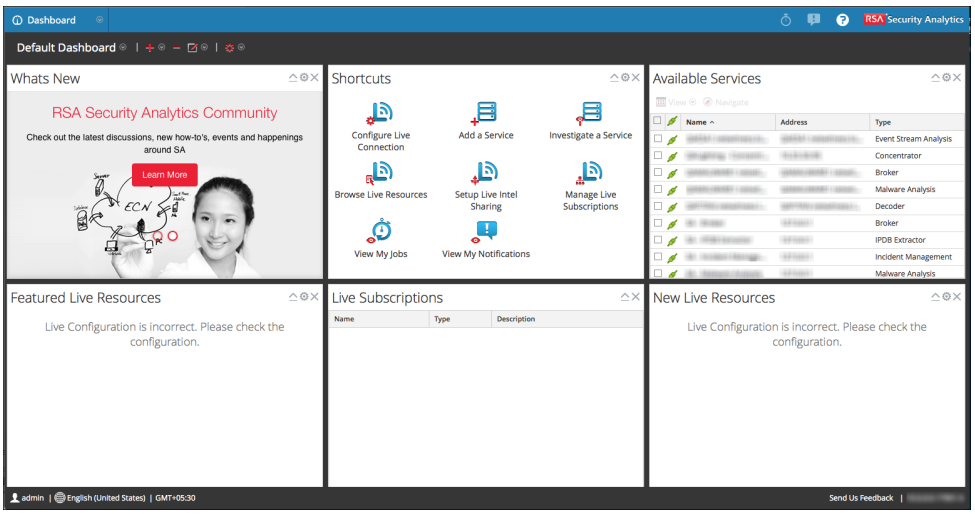
   The Add a Dashlet dialog is displayed.



3. Click on the **Type** selection list to display available types of dashlets, and select the type of dashlet to add.

   Additional configurable fields become available in the **Add a Dashlet** dialog; these vary depending on the dashlet. For example, in an **Reports RE Alert Variance** dashlet, you define the dashlet title, number of alerts, chart type, past hours, and dashlet refresh intervals (minutes). All dashlets have a title.
4. Type a title for the dashlet. You can type letters, numbers, special characters, and spaces for the name. For example, **Service Monitor Dashlet** could be the title.
5. If there are additional configurable fields for the dashlet, set appropriate values. You can select more than one service type.
6. When all required fields have been configured, click **Add**.

   The dashlet is added to the dashboard.



Edit Dashlet Properties

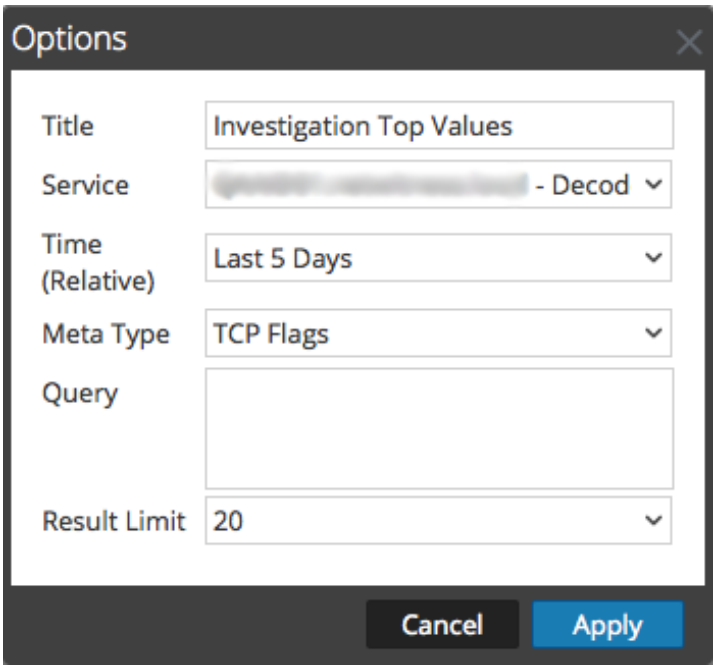
Some dashlets are read-only and properties are not configurable. Other dashlets are configurable to allow users to customize some aspect of the data displayed in that dashlet. A dashlet with editable properties has a settings icon that displays the property sheet for editing.

A dashlet with no editable properties, such as the Live Subscriptions dashlet, does not display the settings icon in the title bar.

Other dashlets have parameters that you define to specify the kind and amount of information you want to see in the dashlet. The custom Investigation Dashboard has three dashlets. Each of the three displays the settings icon.

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

   The **Options** dialog is displayed.



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

   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.

Delete a Dashlet

1. Click the delete control icon ( ) in the dashlet title bar:

   The **Remove Dashlet** dialog asks for confirmation that you want to delete the dashlet.
2. If you want to delete it, click **Yes**. The dashlet is removed from the dashboard.

   If you decide not to delete it, click **No**.

   Note: You cannot delete dashlets associated with the Out-Of-The-Box Dashboard.

Working with Custom Dashboards

To tailor Security Analytics to better serve your site and methods, you can create custom dashboards. Some reasons for creating custom dashboards are:

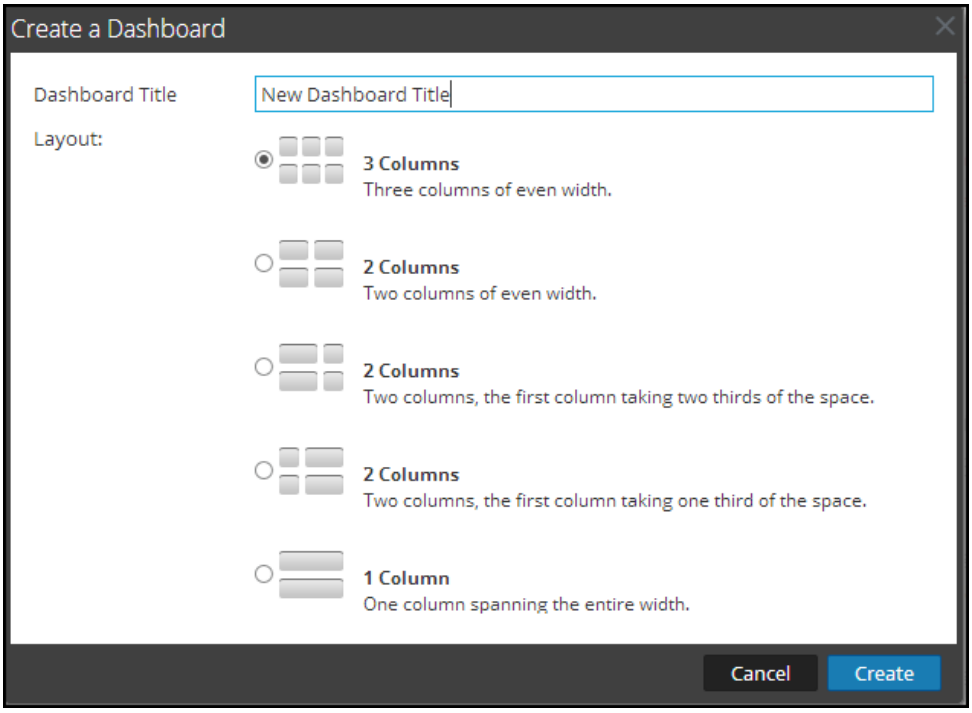
- Consolidate related functionality on a single dashboard.
- Create a Unified dashboard with a collection of dashlets for all modules.
- Create a dashboard to consolidate dashlets for different network locations.
- Create an overview of a given module's capabilities.
- Consolidate dashlets that apply to a specific scenario.

Create a Custom Dashboard

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.

1. In the **Security Analytics** dashboard, select  **> Create New Dashboard**.

   The Create a Dashboard dialog is displayed.



2. Type the title for the new dashboard. You can type letters, numbers, special characters, and spaces for the name. The permitted length of the name is 255 characters.
3. Select a Layout option for the new dashboard.

   The dashboard is created and added to the Dashboard selection list

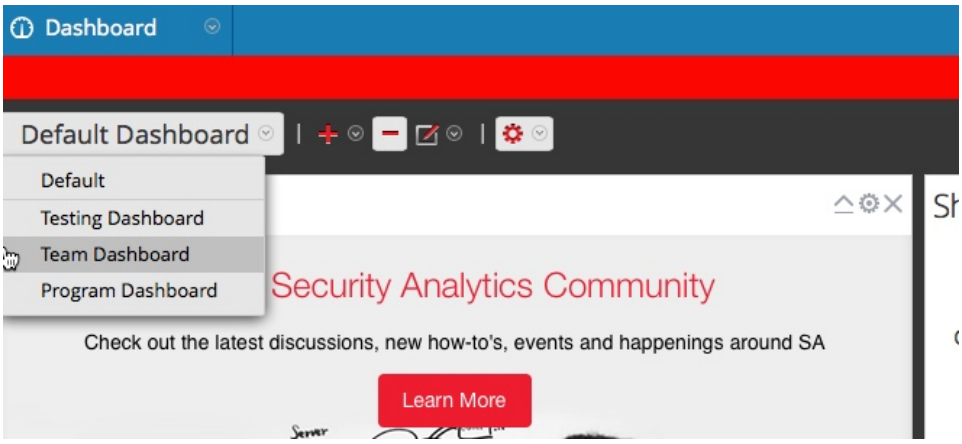
Now that you have created a dashboard, you can:

- Add dashlets to the dashboard.
- Export the dashboard.
- Remove the dashboard.
- Rename the dashboard.

Select a Dashboard

1. To switch between dashboards in a Security Analytics module, click on the **Dashboard Selection List**.

   The Dashboard Selection List is displayed.



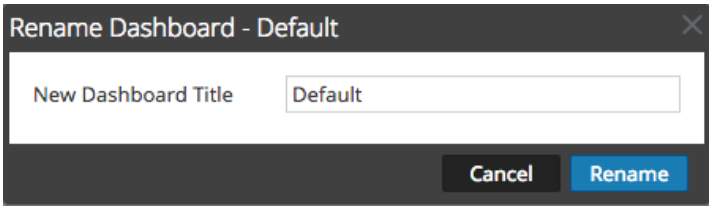
2. Select the dashboard that you want to view.

   The selected dashboard is displayed.

Rename a Custom Dashboard

1. In the dashboard toolbar, select  > **Rename Dashboard**.

   The Rename Dashboard dialog is displayed.



2. In the **New Dashboard Title** field, enter a new title for the dashboard.
3. Click **Rename**.

   The dashboard is updated with the new title.

Remove a Custom Dashboard

If you find that the Dashboard Selection List in Security Analytics includes custom dashboards that are no longer needed, you can remove the unused dashboards. The dashboard to be removed must be displayed. The default and OOTB dashboards cannot be removed.

Note: If you want the dashboard to be available at some future time, you can export the dashboard before removing it as described in Importing and Exporting Dashboards.

1. In the **Dashboard Selection List**, select the unused dashboard; for example, **Region 3**.
   The dashboard is displayed.
2. In the dashboard toolbar, select .
   A dialog asks for confirmation that you want to remove the dashboard.
3. To confirm deletion of the dashboard, click **Yes**.
   The dashboard is removed from the Dashboard Selection List.

Working with Out-Of-The-Box Dashboards

On upgrade, the following Out-Of-The-Box dashboards are available:

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

For more information on each Out-Of-The-Box dashboard, see the OOTB Dashboards.

Features

You cannot perform the following actions on Out-Of-The-Box Dashboard:

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

All the other features available in default and custom dashboards will be applicable in OOTB dashboards.

A dashboard has:

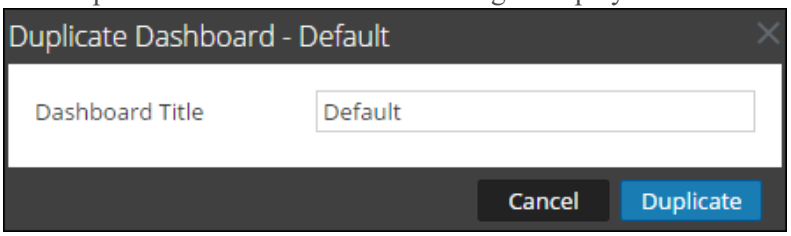
- The dashboard toolbar
- The dashboard title and the Dashboards Selection List.

Copying a Dashboard

To customize the views in Security Analytics, you can copy dashboards to the Security Analytics dashboard or a custom dashboard. The Security Analytics dashboard, as the name suggests, offers all Security Analytics dashlets. The Copy Dashboard dialog creates a duplicate dashboard, the users can modify the duplicate dashboard resulting in a new dashboard. 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 Duplicate Dashboard - Default dialog is displayed.



3. Enter the Dashboard Title.
4. Click Duplicate.

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 Security Analytics.

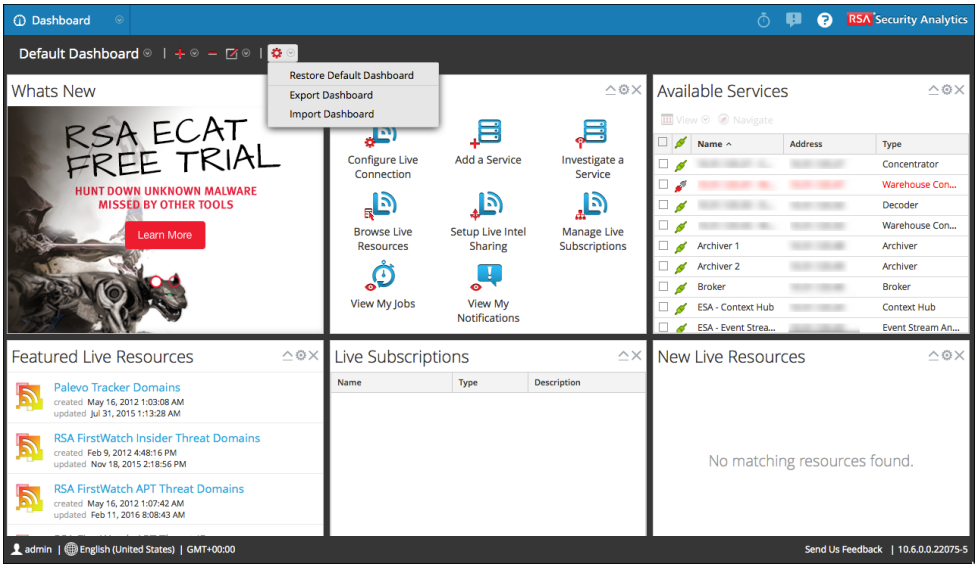
Export a Dashboard

Exported dashboards are designed to work within the same Security Analytics instance. It is also possible to share your custom dashboards with other users in your organization, provided that 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.

Note: When you export the Reporter Realtime Charts dashboard, you must also export the charts used in the Report Realtime Chart dashlets as they are not exported by default. When you import the dashboard, you must manually import the dependent charts used in the Reporter Realtime Chart dashlet.

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.



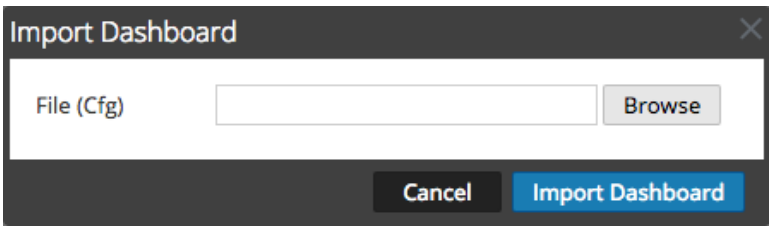
3. A warning appears at the bottom of your screen that downloaded files can harm your computer. If this is the dashboard you wish to export, click **Keep**.
4. Save the exported file in the `.cfg` format.

Note: You cannot export Out-Of-The-Box Dashboards.

Import a Dashboard

Note: You must import the Reporter Realtime Charts dashboard and its related charts into the same instance of the Security Analytics server and Reporting Engine from which it was exported. You must ensure that the data sources configured for the Reporting Engine are the same as on the Security Analytics instance from which it was exported. If you import the dashboard and related charts into another instance of Security Analytics server, you must ensure the data source name is updated in the charts.

1. In the dashboard toolbar, select **Import Dashboard** .



2. Browse to the dashboard file in the **Import Dashboard** dialog. Only `.cfg` files are supported.
3. Click **Import Dashboard**.
   The dashboard is displayed in Security Analytics.

Setting a dashboard as Favorite

To customize the views in Security Analytics, you can set a dashlet as Favorite to the Security Analytics dashboard or a custom dashboard. The Security Analytics dashboard, as the name suggests, offers all Security Analytics dashlets. The Favorite dialog sets a specific dashboard as your favorite dashboard and will load the favorite dashboard everytime you log in to Security Analytics.

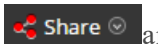
To set a dashboard as Favorite:

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

Sharing a Dashboard

In Security Analytics, you can share dashlets for viewing purposes with other roles such as Administrators, Analysts, Operators and so on. The Security Analytics dashboard, as the name suggests, offers all Security Analytics dashlets. When you share a dashlet, the users can only view the dashboard, make dashboard as favorite, copy the dashboard, and eport the dashboard. The user will be able to share their dashboard with the roles that they belong to. For example, an analyst will be able to share his dashboard with other analysts only.

To share a dashboard:

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.

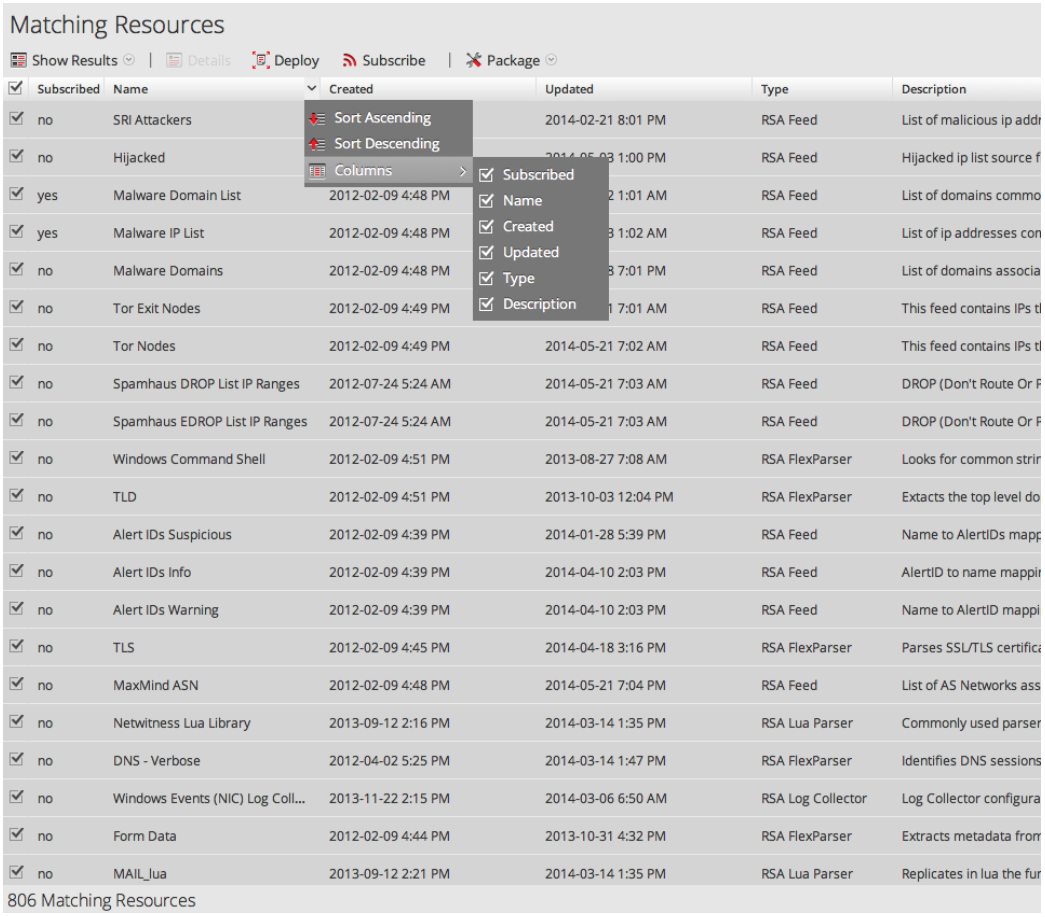
Note: If you do not want to share the dashboard, clear the checkbox of the role.

Configuring Grids

Much of the information displayed in the Security Analytics dashboards and dashlets is best displayed in rows and columns. This is called a grid, and all grids can be customized in several ways. You can:

- Select which columns to display.
- Sort each column in ascending or descending order
- Change the width of columns.

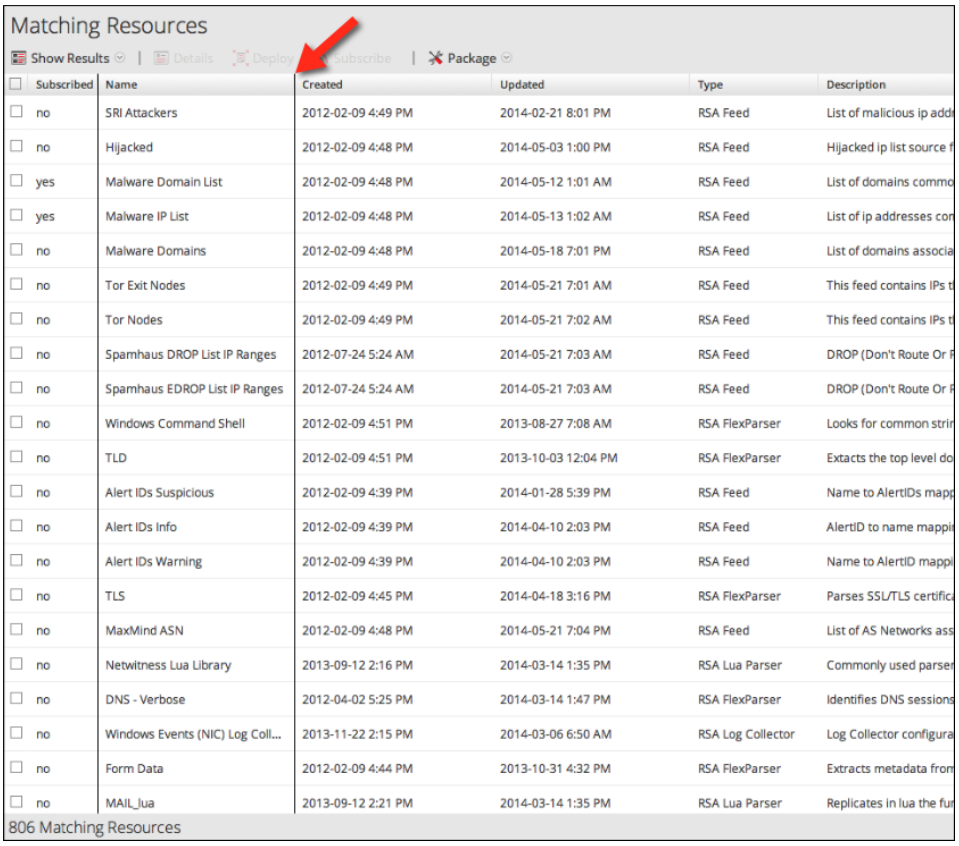
This is an example of a grid (the Live Search View's Matching Resources grid).



Change the Column Width

You can change the width of a column to make columns narrower or wider than they are by default. For example, if a column is too narrow to display all of its contents, you can widen it.

1. Hover in the title bar on the right edge of the title.
2. When the cursor changes to the column resize cursor (one short vertical line with arrows pointing right and left), click and drag the line to make the column wider or narrower. This is an example of resizing the Name column in progress.



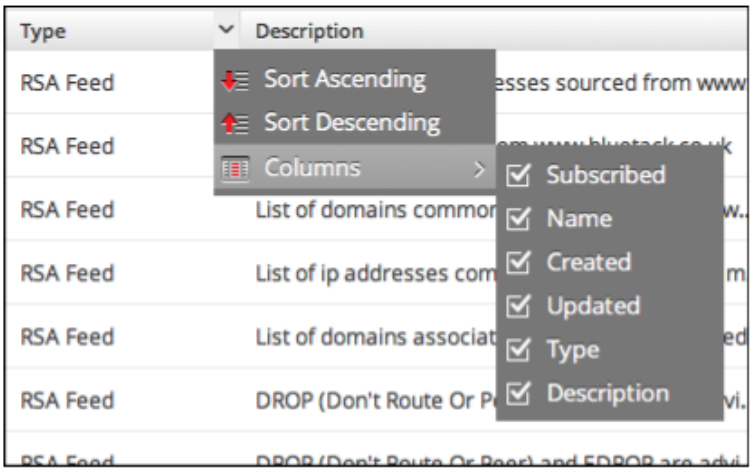
Subscribed	Name	Created	Updated	Type	Description
no	SRI Attackers	2012-02-09 4:49 PM	2014-02-21 8:01 PM	RSA Feed	List of malicious ip add
no	Hijacked	2012-02-09 4:48 PM	2014-05-03 1:00 PM	RSA Feed	Hijacked ip list source f
yes	Malware Domain List	2012-02-09 4:48 PM	2014-05-12 1:01 AM	RSA Feed	List of domains commo
yes	Malware IP List	2012-02-09 4:48 PM	2014-05-13 1:02 AM	RSA Feed	List of ip addresses cor
no	Malware Domains	2012-02-09 4:48 PM	2014-05-18 7:01 PM	RSA Feed	List of domains associa
no	Tor Exit Nodes	2012-02-09 4:49 PM	2014-05-21 7:01 AM	RSA Feed	This feed contains IPs t
no	Tor Nodes	2012-02-09 4:49 PM	2014-05-21 7:02 AM	RSA Feed	This feed contains IPs t
no	Spamhaus DROP List IP Ranges	2012-07-24 5:24 AM	2014-05-21 7:03 AM	RSA Feed	DROP (Don't Route Or F
no	Spamhaus EDROP List IP Ranges	2012-07-24 5:24 AM	2014-05-21 7:03 AM	RSA Feed	DROP (Don't Route Or F
no	Windows Command Shell	2012-02-09 4:51 PM	2013-08-27 7:08 AM	RSA FlexParser	Looks for common strir
no	TLD	2012-02-09 4:51 PM	2013-10-03 12:04 PM	RSA FlexParser	Extacts the top level do
no	Alert IDs Suspicious	2012-02-09 4:39 PM	2014-01-28 5:39 PM	RSA Feed	Name to AlertIDs mapp
no	Alert IDs Info	2012-02-09 4:39 PM	2014-04-10 2:03 PM	RSA Feed	AlertID to name mappi
no	Alert IDs Warning	2012-02-09 4:39 PM	2014-04-10 2:03 PM	RSA Feed	Name to AlertID mappi
no	TLS	2012-02-09 4:45 PM	2014-04-18 3:16 PM	RSA FlexParser	Parses SSL/TLS certific
no	MaxMind ASN	2012-02-09 4:48 PM	2014-05-21 7:04 PM	RSA Feed	List of AS Networks ass
no	Netwitness Lua Library	2013-09-12 2:16 PM	2014-03-14 1:35 PM	RSA Lua Parser	Commonly used parser
no	DNS - Verbose	2012-04-02 5:25 PM	2014-03-14 1:47 PM	RSA FlexParser	Identifies DNS sessions
no	Windows Events (NIC) Log Coll...	2013-11-22 2:15 PM	2014-03-06 6:50 AM	RSA Log Collector	Log Collector configura
no	Form Data	2012-02-09 4:44 PM	2013-10-31 4:32 PM	RSA FlexParser	Extracts metadata fron
no	MAIL_lua	2013-09-12 2:21 PM	2014-03-14 1:35 PM	RSA Lua Parser	Replicates in lua the fu

3. When the width is correct, release the mouse button.

Select Which Columns to Display

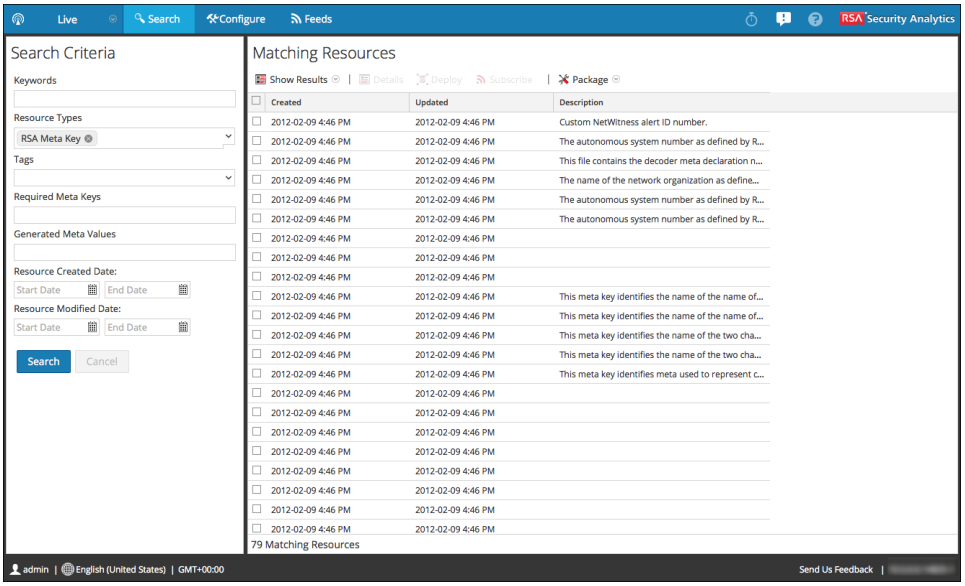
1. Hover in the title bar on the right edge of the title.
2. When the cursor changes to the selection list icon ( ), click to see the list.
3. At the bottom of the list, select **Columns**.

A list of available columns is displayed with a check mark for each column currently included in the grid.



4. Select a column name to select or deselect it.

   When you deselect a column name, that column is removed from the grid. When you select a column name, that column is added to the grid. This is an example of the Matching Resources grid after several columns are deselected.



Sort the Contents of a Column

To tailor a grid to better serve your purpose, you can choose how the contents of each grid column are sorted.

1. Hover in the title bar on the right edge of the title.
2. When the cursor changes to the selection list icon ( ) click to see the menu.

The menu displays a list of available sort options.

3. Select from the sort options; for example, Sort Ascending or Sort Descending.

   The grid is sorted based on your selection.

Managing Jobs

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

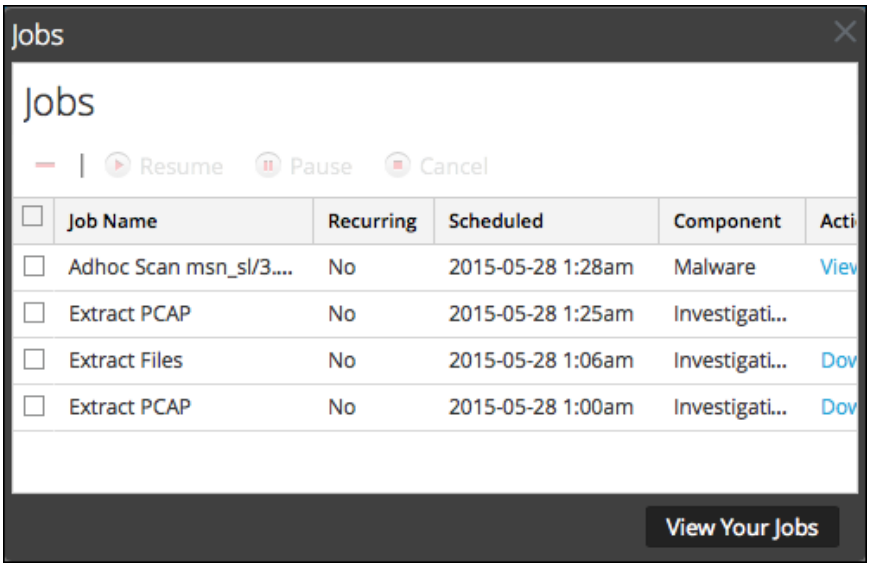
- In the Profile view, you see the same jobs in a full panel. These are only your jobs.
- In the System view, users with administrative privileges can view and manage all jobs for all users in a single jobs panel.

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

Display the Jobs Tray

In the **Security Analytics** toolbar, click the Jobs icon:  .

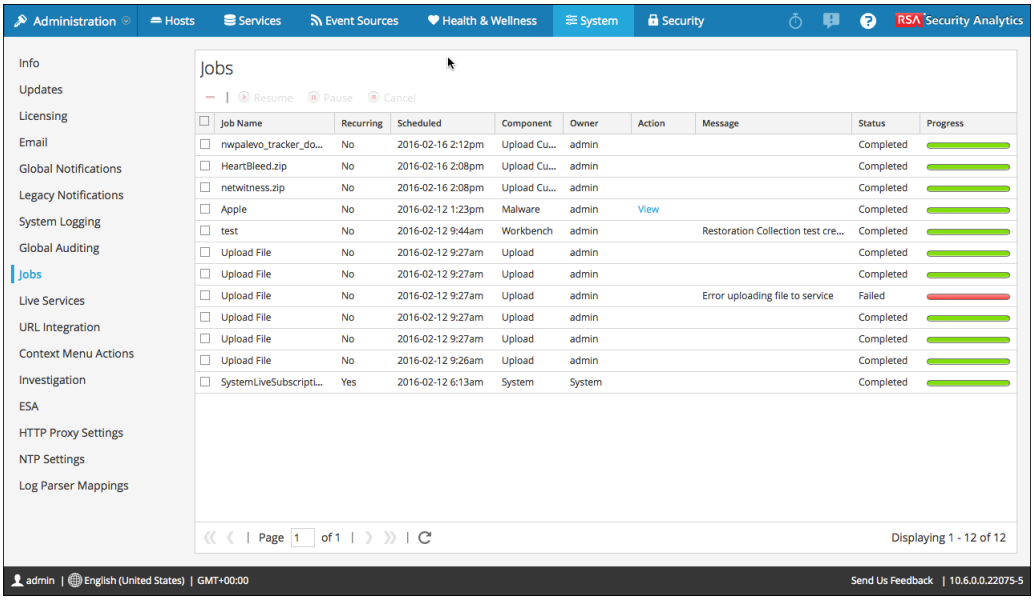
The Jobs Tray is displayed.



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 Profile view > Jobs panel are the same. In the Administration System view, the Jobs panel lists information about all Security Analytics jobs for all users.

View 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. Users with the ADMIN role 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 Investigation Module 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 Security Analytics, 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 Security Analytics toolbar. You can look anytime, but when a new notification is received, the Notifications icon is flagged.

Examples of notifications include:

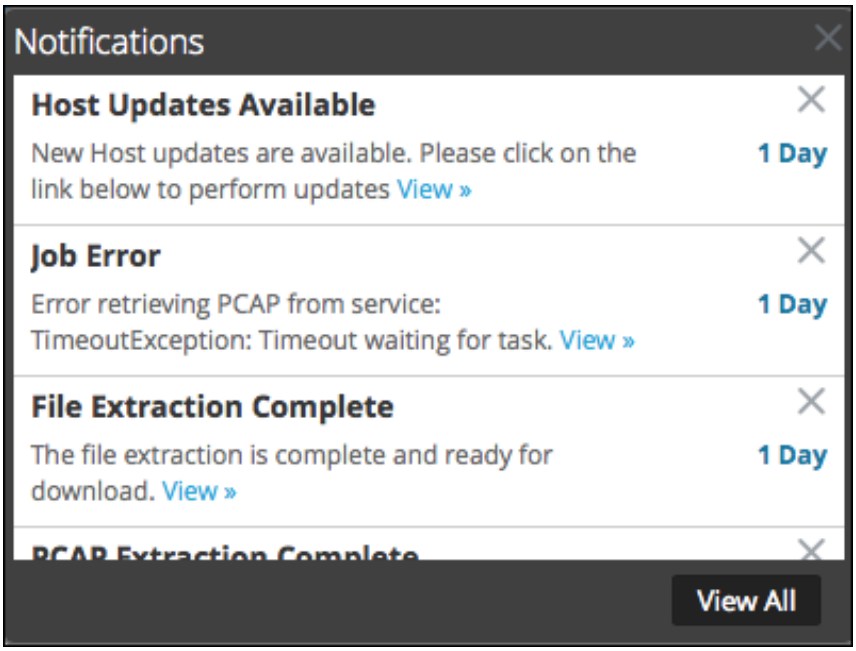
- A host upgrade completed.
- A parser push to decoders completed.
- A newer software version is available.

You can see all notifications in a full Notifications panel in these two views.

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

View Notifications

To display the Notifications tray, in the Security Analytics toolbar, click the Notifications icon ().



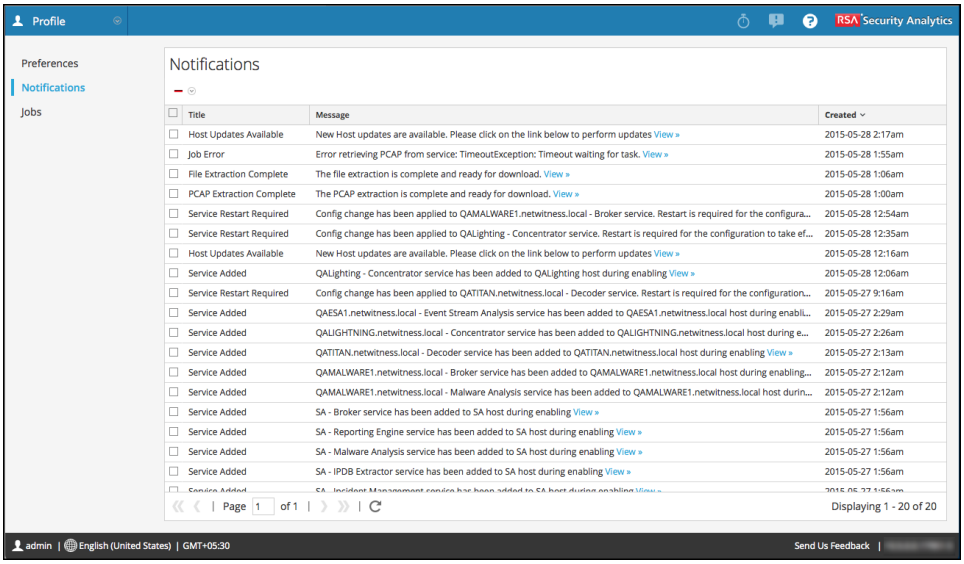
View All Notifications

To view all notifications, do one of the following:

1. In the **Security Analytics** menu, select **Profile**, then in the options panel of the **Profile** view, select **Notifications.**
2. In the **Security Analytics** menu, select **Administration > System**, then in the options panel of the System view, select **Notifications.**
3. In the **Security Analytics** toolbar, click  to open the Notifications tray, then click **View All** in the Notifications tray.

   The Notifications panel is displayed. Here all notifications are displayed, and the format is

different from the format of the Notifications Tray.



Delete Notification Records

To delete notification records:

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

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

Getting Started with Security Analytics: References

The Security Analytics user interface includes features such as:

- Profile View > Preferences Panel
- Notifications Panel and Notifications Tray
- Jobs Panel and Jobs Tray
- Admin News Dashlet
- Admin Service List Dashlet
- Dashboard RSA First Watch Dashlet
- Dashboard Shortcuts Dashlet
- Dashboard What's New Dashlet
- Incidents Analysts Activity Dashlet
- Incidents Queue Activity Dashlet
- Investigation Jobs Dashlet
- Investigation Top Values Dashlet
- Live Featured Resources Dashlet
- Live New Resources Dashlet
- Live Subscriptions Dashlet
- Live Updated Resources Dashlet
- Malware Malware with High Confidence IOCs and High Scores Dashlet
- Malware Scan Jobs List Dashlet
- Malware Top Listing of Possible Zero Day Malware Dashlet
- Malware Top Listing of Highly Suspicious Malware Dashlet
- Reports Realtime Chart Dashlet
- Reports RE Alert Variance Dashlet
- Reports Recent Run Report Dashlet

- Reports RE Recent Alerts Dashlet
- Reporting RE Top Alerts Dashlet

This section includes an example of each one. You may find the examples of dashlets useful when deciding how to customize your dashboards.

Jobs Panel and Jobs Tray

Jobs are started by various Security Analytics 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 Security Analytics jobs in the Jobs panel. Other non-administrative users can view their own jobs in the Profile view.

In addition, while working in Security Analytics, you can open a quick view of your jobs from the Security Analytics 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.

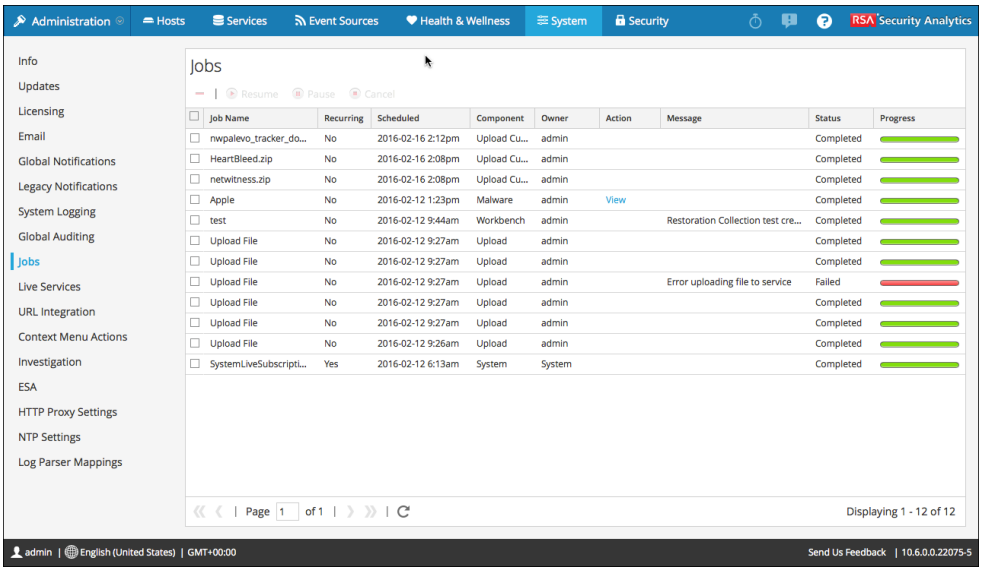
In the Jobs panel, you can:

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

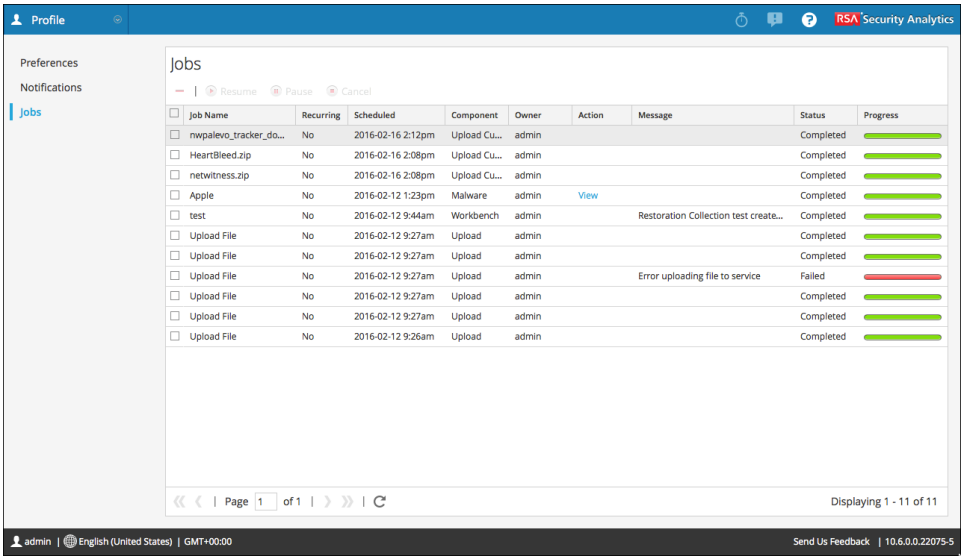
The structure of the jobs panel is the same in all views. Procedures associated with the Jobs panel and Jobs tray are described in Managing Jobs.

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

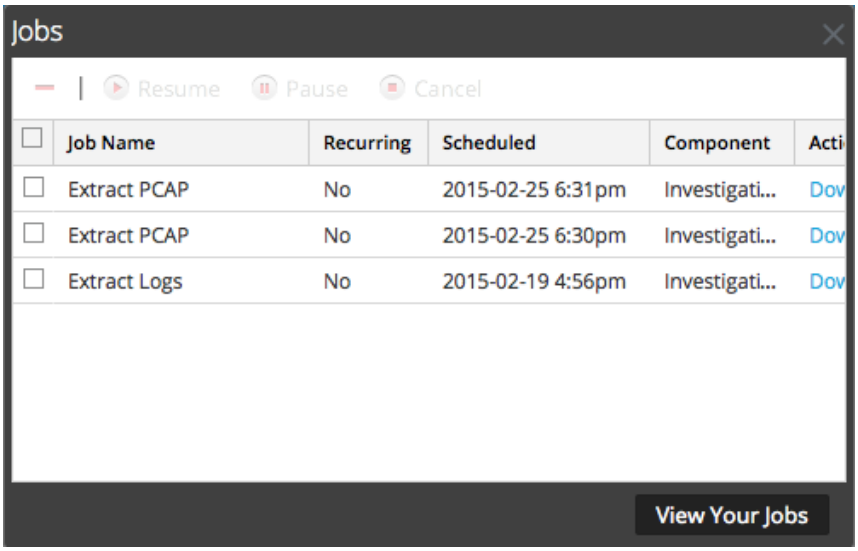
- In the **Security Analytics** menu, select **Administration > System**, and in the options panel, select **Jobs**.



- In the **Security Analytics** menu, select **Profile**, and in the options panel, select **Jobs**.



To display the Jobs tray, in the Security Analytics toolbar, click the **Jobs** icon  .



The Jobs panel organizes information about jobs into a grid. The columns present a job progress bar, the job name, an indication that the job is recurring or not recurring, the Security Analytics 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.

Features

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 Administration System view, the Jobs panel lists information about all Security Analytics jobs for all users.

This table lists the toolbar 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.

This 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.**
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.

Feature	Description
View Your Jobs	Displays jobs in the **Profile View > Jobs panel.**
Scheduled	Indicates the date and time at which the job was scheduled to begin.

Notifications Panel and Notifications Tray

Security Analytics 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.

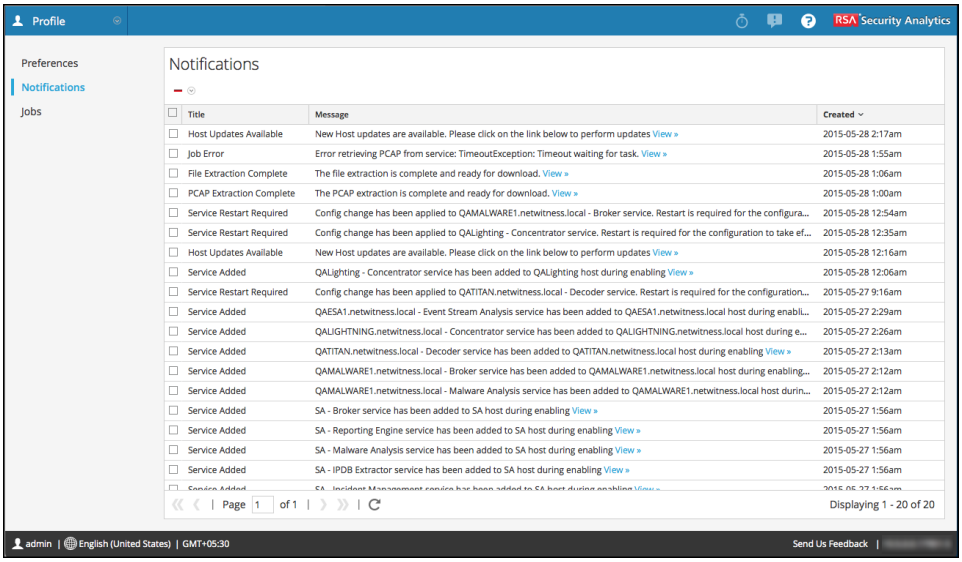
While you are working in Security Analytics, you can view recent system notifications without leaving the module in which you are working. You can open a quick view of notifications from the Security Analytics toolbar. You can look anytime, but when a new notification is received, the Notifications icon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

When you are viewing notifications in the Notifications tray, only recent notifications are displayed. You can view all notifications in a grid format in the Profile view or in the System view. Procedures for viewing notifications are provided in Viewing and Deleting Notifications.

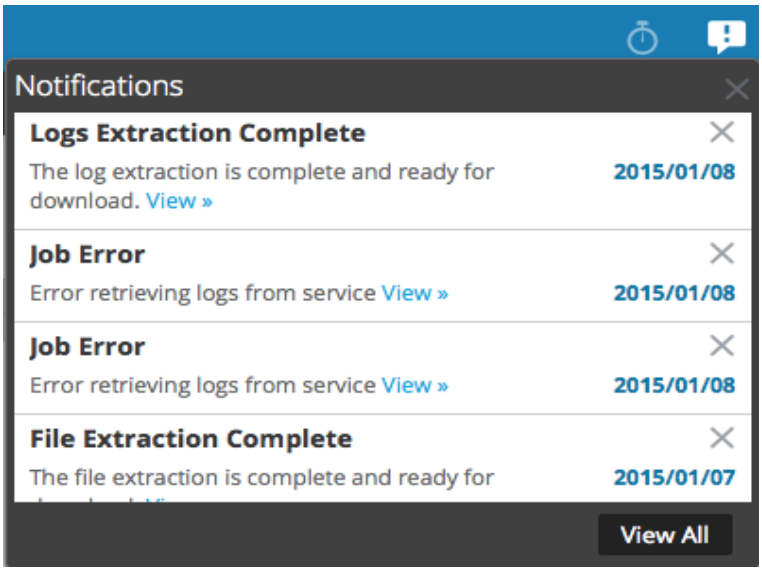
To access the Notifications panel, do one of the following:

- In the **Security Analytics** menu, select **Profile**, then in the options panel of the Profile view, select **Notifications.**

- In the **Security Analytics** menu, select Administration > System, then in the options panel of the System view, select **Notifications.**



- In the **Security Analytics** toolbar click  , then click **View All** in the Notifications tray.



Features

The Notifications panel and tray has a toolbar and a grid. The Notification tray is a subset of the information in the Notifications panel. The following table describes the Notifications panel features.

Feature	Description
	Displays a drop-down menu where you can delete the selected notification records or all the notification records in the **Notifications** grid 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 link that displays a view where you can take action. For example, if there is a file to download, clicking this link opens the Jobs panel, the view where you can download the file.
Created	The date and time the notification was created. In the Notifications Tray, this column is the number of days since the notification was created.
View All	Displays the Profile View Notifications Grid.

Profile View > Preferences Panel

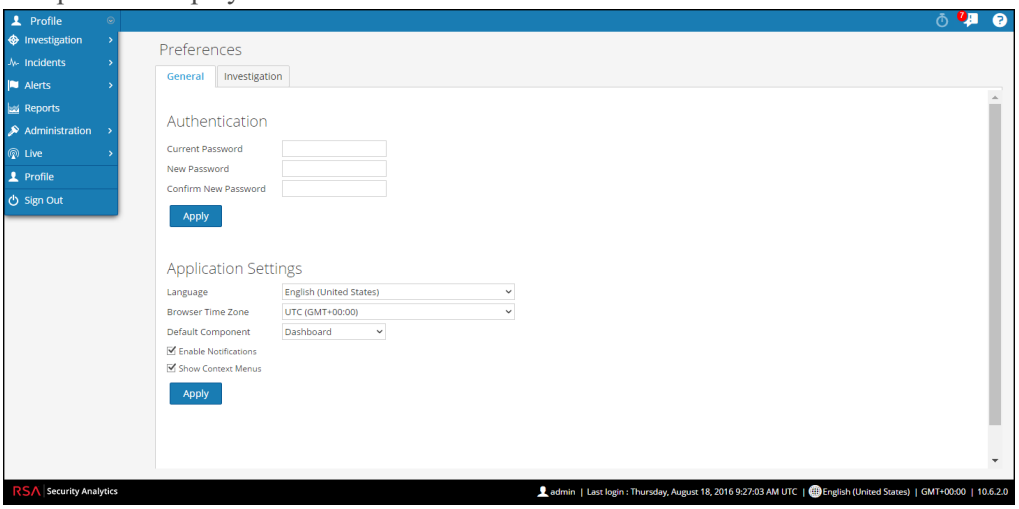
Users can set several preferences that are applied on top of system preferences set by the System Administrator. These include:

- General preferences for Security Analytics and settings for the Security Analytics application as a whole (described below)
- Preferences that apply to Investigation and can affect initial views and load time
- Preferences that apply to Reporter.

To access this panel:

1. In the **Security Analytics** menu, select **Profile**.
2. In the options panel of the **Profile** view, select **Preferences**.

   The panel is displayed with the General tab selected.



Features

The Preferences panel > General tab has two sections: Authentication and Application Settings.

Authentication

The following table describes options in the Authentication section. The related procedure is described in Changing Your Password.

Feature	Description
Current Password	Enter your current password that you used to log in to Security Analytics.
New Password	Enter the password that you want to use from the next login . The password must be at least 8 characters in length, and can include uppercase and lowercase letters, numbers, special characters, and spaces.
Confirm Password	Confirm Password Re-enter the new password to confirm.
Apply	Updates your user profile with the new password. The new password becomes effective immediately and is required the next time you log on to Security Analytics. The password change is applied to your system log on and to all Security Analytics services on which your account has been added.

Application Settings

The following table describes options in the Application Settings section. Related procedures are described in Configuring Application Preferences.

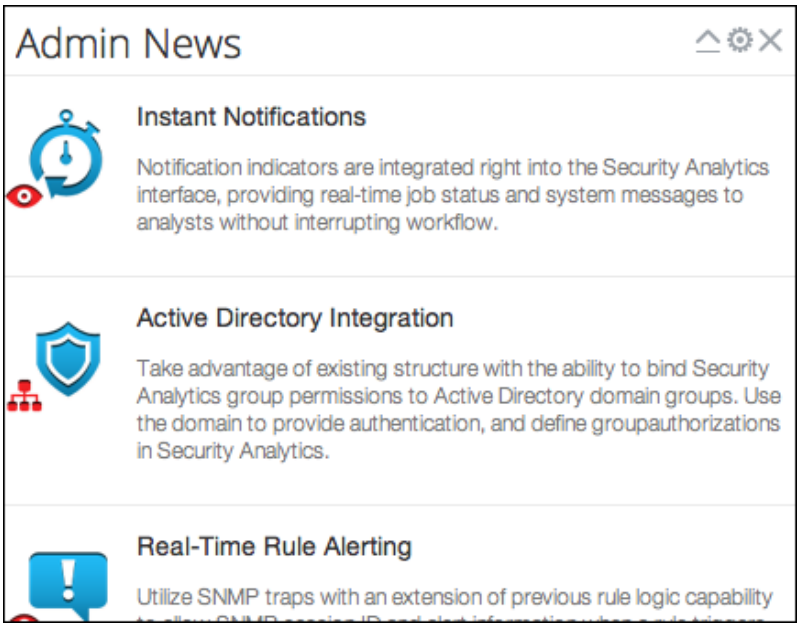
Feature	Description
Language	Displays a drop-down list of languages available to use in Security Analytics.
Browser Time Zone	Displays a drop-down list of time zones available to use in Security Analytics.
Default Component	This field has a drop-down list for selecting the component that serves as the opening view when you log on to Security Analytics.
Enable Notifications	This checkbox enables and disables notifications for your user account. By default, Security Analytics system notifications are enabled when a new user account is created.

Feature	Description
Show Context Menus	This checkbox enables and disables context menus for your user account. By default, Security Analytics 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 the application settings and the changes are applied immediately.

Admin News Dashlet

This dashlet presents product information and updates for the Administration module.

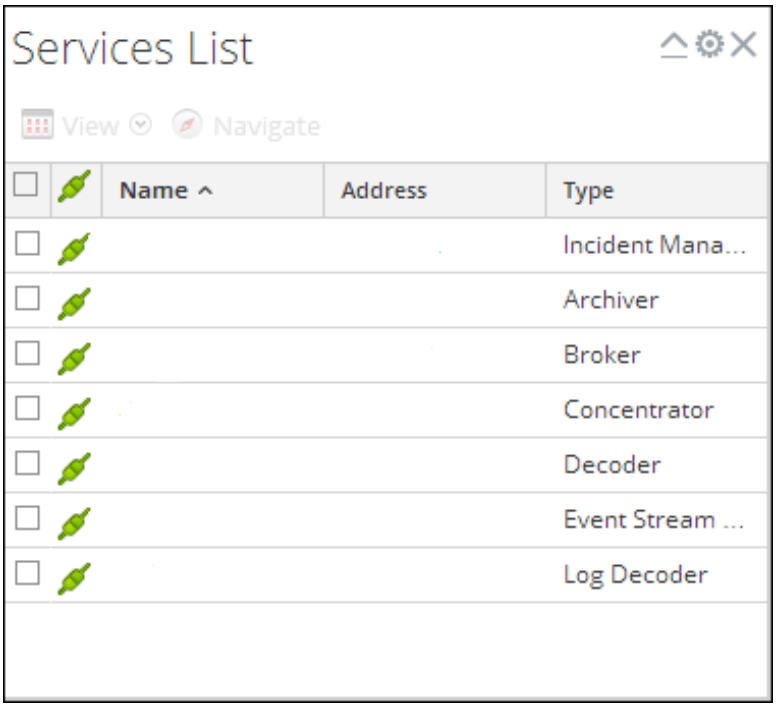
To display this dashlet in the Security Analytics dashboard or as part of a custom dashboard, in the dashboard toolbar, select > **Add a Dashlet** in the dashboard and select **Admin News.**



Admin Service List Dashlet

The Administration Service List dashlet is a list of available services in Security Analytics with links to administrative tasks that can be taken on those services. In effect, this dashlet is a focused subset of the **Administration Hosts View** (see the topic in the *Hosts and Services Getting Started Guide*.

To display this dashlet in the Security Analytics dashboard or as part of a custom dashboard, select > **Add Dashlet** in the dashboard toolbar and select **Admin Services List**.



Features

- The View menu ( ) option is a quick link to the View menu in the Administration Services view. Select a service and click here to select a view.
- The Navigate option is a quick link to the Navigate view in the Investigation module.
- The Services grid has a subset of the grid columns in the Administration Hosts view. The following table provides descriptions of the columns presented in the dashlet

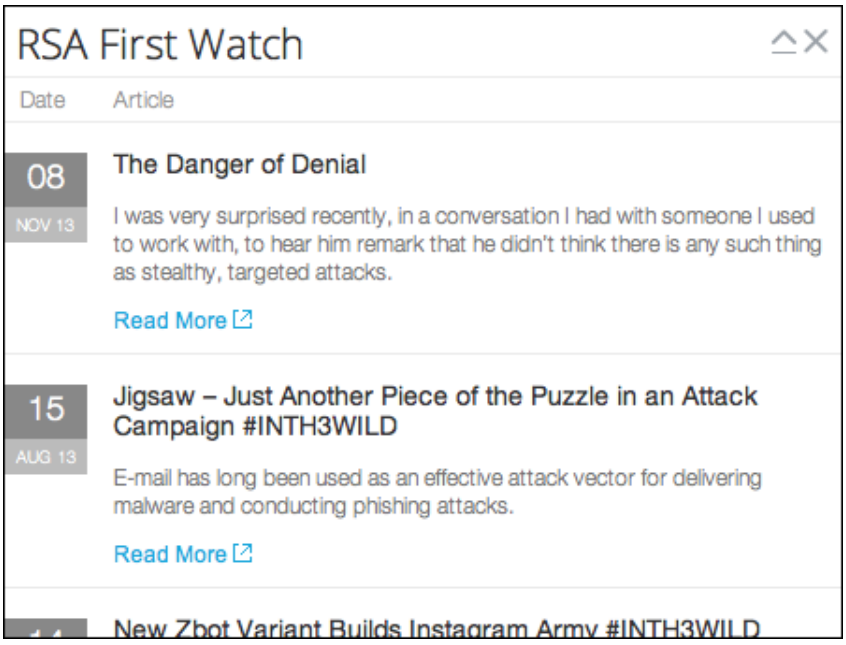
Column	Description
	Selection checkbox. Click in the heading to select or deselect all services in the list.
Connection Status	The connection icons indicate whether the connection to the service is good (green) or bad (red and gray). Rendering of the entire row in red text also reflects a bad connection status.
Name	The name of the service; for example **HQ-Decoder** or **10.26.22.44-Decoder**.

Column	Description
Address	The IP address of the NextGen service; for example, **10.26.22.44**.
Type	The type of service. Possible values are Broker, Concentrator, Decoder, Log Decoder, Log Collector, Archiver, Workbench, Warehouse Collector, Event Stream Analysis, IPDB Extractor, Reporting Engine, Malware Analysis, and Incident Management.

Dashboard RSA First Watch Dashlet

The Dashboard RSA First Watch dashlet delivers situational awareness and threat intelligence from across the RSA research and incident-response community, providing customers the intelligence to prepare for, respond to, and mitigate advanced cyber threats. The RSA First Watch, Incident Response, and Computer Incident Response Center (CIRC) teams track millions of IPs and domains, as well as dozens of unique threat sources and threat actors.

To display this dashlet in the Unified dashboard or as part of a custom dashboard, click  > **Add Dashlet** in the dashboard toolbar and select **Dashboard RSA First Watch**.



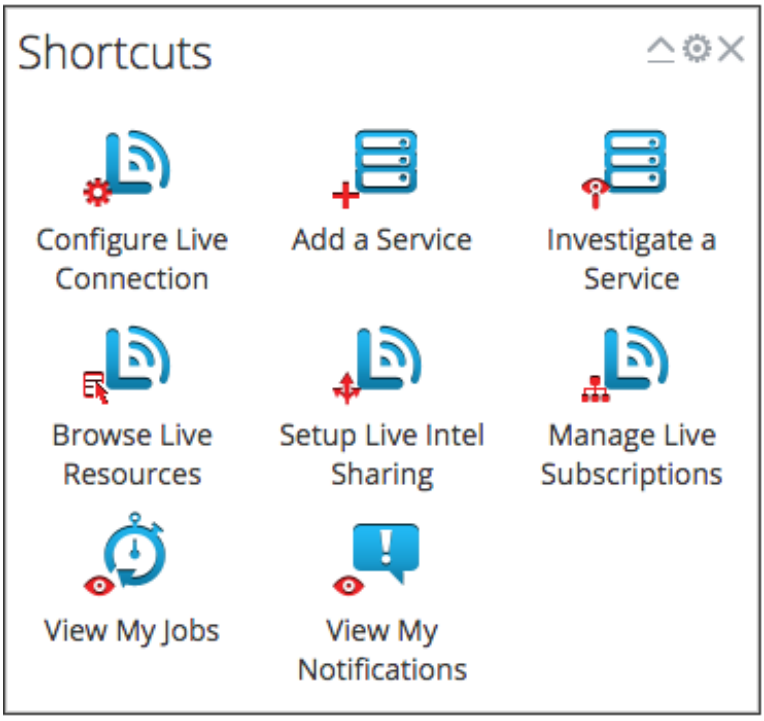
Features

Column	Description
Date	The date the article was posted.
Article	The article title, a sample of the article, and a "Read More" link to the full article.

Dashboard Shortcuts Dashlet

The Dashboard Shortcuts dashlet offers quick links to common tasks in other areas of Security Analytics. It is a good tool for first-time users who are trying to get a feel for the system.

To display this dashlet in the Security Analytics dashboard or as part of a custom dashboard, click  > **Add Dashlet** in the dashboard toolbar and select the **Dashboard Shortcuts** dashlet.



Features

In addition to the standard dashlet controls, this dashlet has options that link to common Security Analytics tasks.

Option	Description
Configure Live Connection	Links to the Administration System View > Live Configuration Panel, where you configure the connection to the Live content management system.
Add a Service	Links to the Services View.

Option	Description
Investigate a Service	Links to the Navigate View Navigate Tab, in which you can select a service to navigate from a list of available services.
Browse Live Resources	Links to the Live Search View, in which you search the Live resource library for resources.
Setup Live Intel Sharing	Links to the Administration System View, in which you can choose to participate in live intelligence sharing.
Manage Live Subscriptions	Links to the Live Configure View, in which you view and edit subscriptions and deployments.
View My Jobs	Links to the Jobs Panel (Profile View), in which you view Security Analytics jobs.
View My Notifications	Links to the Notifications Panel (Profile View), in which you view system notifications.

Dashboard What's New Dashlet

The Dashboard What's New dashlet displays the latest product information and announcements for all Security Analytics products.

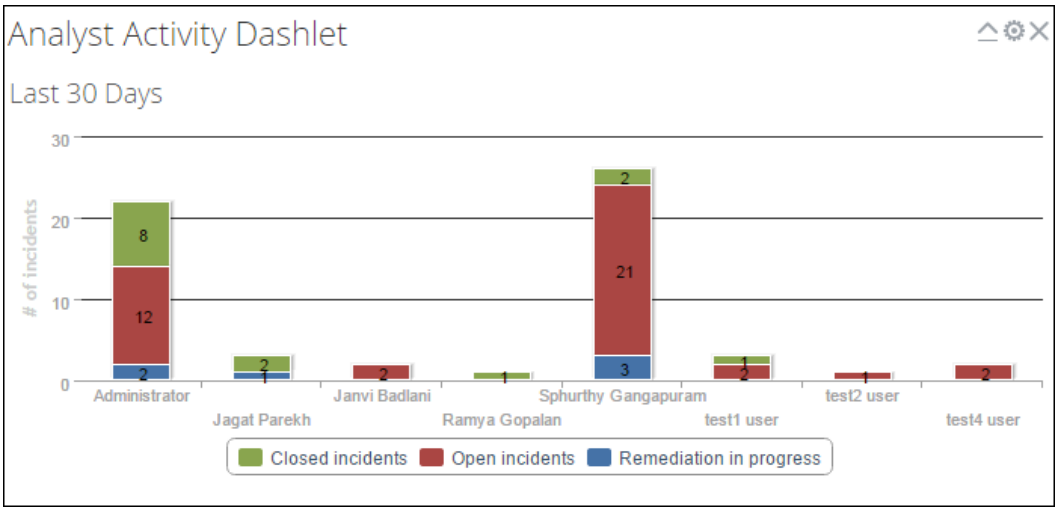
To display this dashlet in the Security Analytics dashboard or as part of a custom dashboard, click  > **Add Dashlet** in the dashboard toolbar and select **Dashboard What's New** dashlet.

Incidents Analysts Activity Dashlet

The Incidents Analysts Activity dashlet shows the number and status of incidents per analyst, over a range of time. It displays three categories:

- Closed incidents
- Open incidents
- Remediation in progress

To display this dashlet in the Security Analytics dashboard or as part of a custom dashboard, click > **Add Dashlet** in the dashboard toolbar. Select **Incidents Analysts Activity** from the drop-down menu and set a time range for the activity.



Note: When you collapse the dashlet using the option, the bars take some time to redisplay. You can refresh the browser to see the graph quickly.

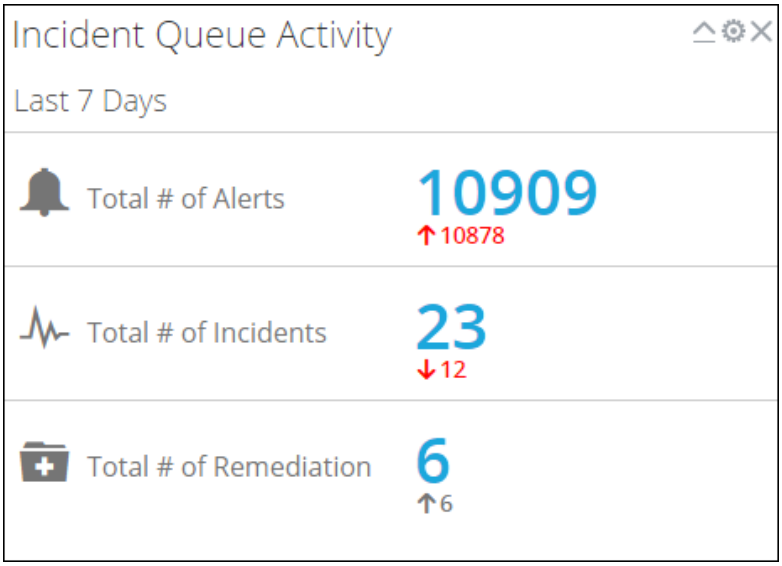
Feature	Description
Bar graph	When you hover the mouse over a portion of the bar graph, the number and status of incidents is displayed in text.
Incident categories	In the legend at the bottom, incident categories are displayed. Clicking a category removes it from the graph. Clicking the category again redisplays it in the graph.

Incidents Queue Activity Dashlet

The Incidents Queue Activity dashlet displays the total number of alerts, incidents, and remediation tasks for a selected time range.

To display this dashlet on the Security Analytics dashboard or as part of a custom dashboard, click > **Add Dashlet** in the dashboard toolbar and select **Incidents Queue Activity**. In the Add a Dashlet dialog, enter a title for the dashlet and select a time range for results.

The figure below is an example of the dashlet with information from the last 7 days.

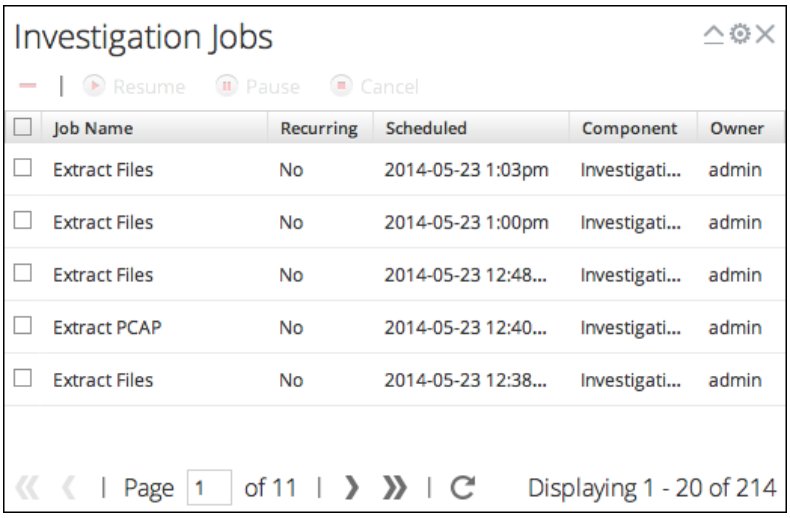


Feature	Description
Totals	Separate rows display the totals of alerts, incidents, and remediation. Clicking a total opens the respective tab for alerts, incidents, or remediation.
Increase and Decrease	The number below the total is the amount of increase or decrease. A total that has changed more than 33% is in red. A total that has changed less than 33% is in gray.

Investigation Jobs Dashlet

The Investigation Jobs dashlet displays the status of all jobs in the Investigation module. The toolbar, grid, and job management procedures are described under Jobs Tray.

To display this dashlet in the default dashboard or as part of a custom dashboard, click > **Add Dashlet** in the dashboard toolbar and select **Investigation Jobs**.



Features

The Investigation Jobs dashlet lists all jobs that you own, recurring and non-recurring, and lets you monitor their progress.

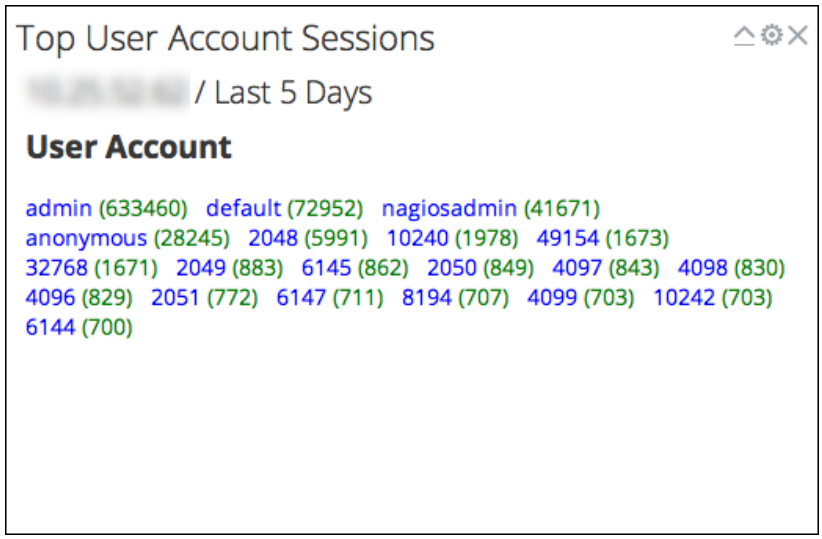
Feature	Description
Resume	The Resume option applies only to recurring jobs that have been paused. When you resume a paused job, the next execution of the job executes as scheduled.
Pause	The Pause option applies only to recurring jobs. When you pause a recurring job that is running, it has no effect 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.

Investigation Top Values Dashlet

The Investigation Top Values dashlet allows you to inspect the top values for a specific time period and for a specific meta type on a given appliance. You define the meta data and query parameters in the Add a Dashlet dialog.

To display this dashlet in the Security Analytics dashboard or as part of a custom dashboard, click > **Add Dashlet** in the dashboard toolbar and select **Investigation Top Values**.



Features

You define the meta data and query parameters in the **Add a Dashlet** dialog.

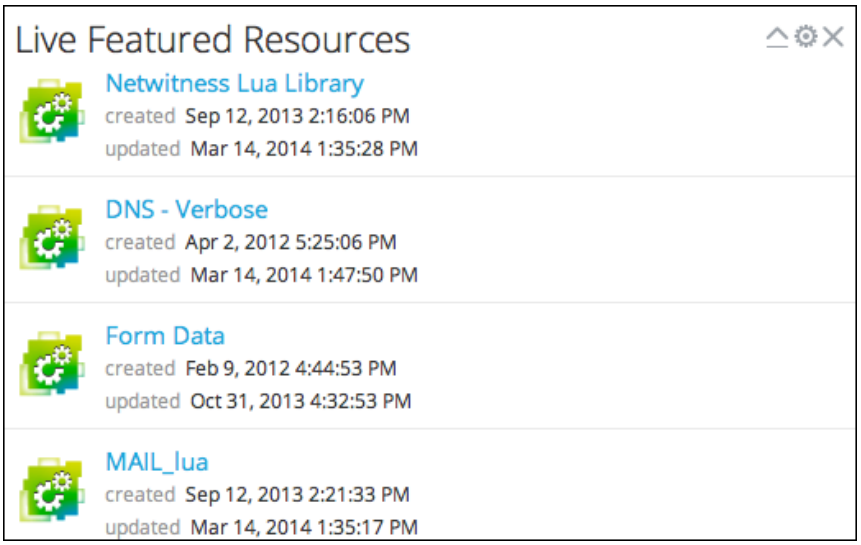
Feature	Description
Title	The title of the dashlet.
Service	The name or IP address of the target service.

Feature	Description
Time (Relative)	Last 5 minutes Last 10 minutes Last 15 minutes Last 30 minutes Last Hour Last 3 Hours Last 6 Hours Last 12 Hours Last 24 Hours Last 2 Days Last 5 Days
meta Type	Select the meta type from the drop-down list.
Query	Complete the query to further define the results
Result Limit	Select the number of results to display from the drop-down list.

Live Featured Resources Dashlet

The Live Featured Resources dashlet displays the list of Live resources that are tagged as featured for the configured Content Management System (CMS) server.

To display this dashlet in the Security Analytics dashboard or as part of a custom dashboard, click  > **Add Dashlet** in the dashboard toolbar and select **Live Featured Resources**.



Features

This dashlet has a paged view of featured Live resources and provides the following information about each resource.

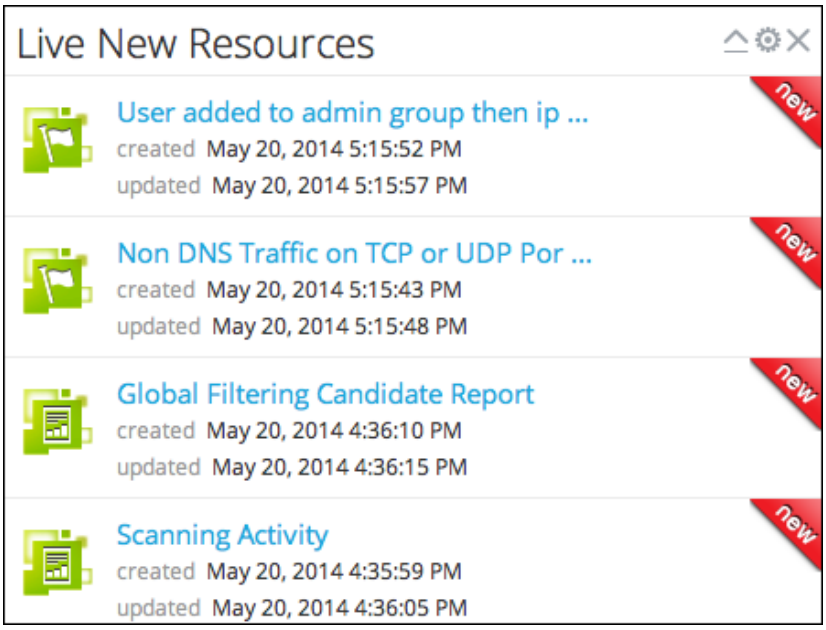
Value	Description
 (Resource Type Icon)	Each type of Live resource is represented by an icon. For example, the icon in the screen capture represents a Parser feed. Clicking the Resource Type icon opens a new browser tab with the detailed view of the resource in the Live Resource view.
Resource Name	The name of the resource, for example, **NetWitness APT Threat IPs**. Clicking the **Resource Name** displays the detailed view of the resource in the Live Resource view. The view opens in the current browser tab.
Date Created	The date the resource was created.

Value	Description
Last Updated Date	The date the resource was last updated.

Live New Resources Dashlet

The Live New Resources dashlet displays a list of Live CMS resources that are tagged as new for the configured Content Management System (CMS) server. You can click a resource name to go to the detailed view of the resource.

To display this dashlet in the Security Analytics dashboard or as part of a custom dashboard, click > **Add Dashlet** in the dashboard toolbar and select **Live New Resources**.



Features

This dashlet has a paged view of new Live resources and provides the following information about each resource.

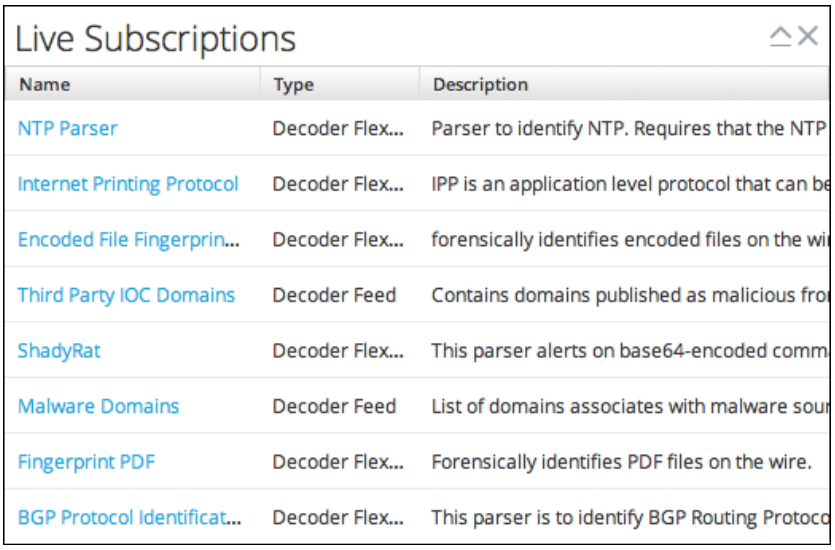
Value	Description
 Resource Type Icon	Each type of Live resource is represented by an icon. For example, the icon to the left represents a Decoder FlexParser. Clicking the Resource Type icon opens a new browser tab with the detailed view of the resource in the Live Resource view.

Value	Description
Resource Name	The name of the resource, for example, **Gh0st Protocol Parser**. Clicking the Resource Name displays the detailed view of the resource in the Live Resource view. The view opens in the current browser tab.
Date Created	The date the resource was created.
Last Updated Date	The date the resource was last updated.

Live Subscriptions Dashlet

The Live Subscriptions dashlet presents a listing of all Live resources to which this Security Analytics instance is subscribed. This is simply a quick reference list. If you need to manage subscriptions, use the Subscriptions Tab in the Live Manage view.

To display this dashlet in the Security Analytics dashboard or as part of a custom dashboard, click  > **Add Dashlet** in the dashboard toolbar and select **Live Subscriptions**.



Features

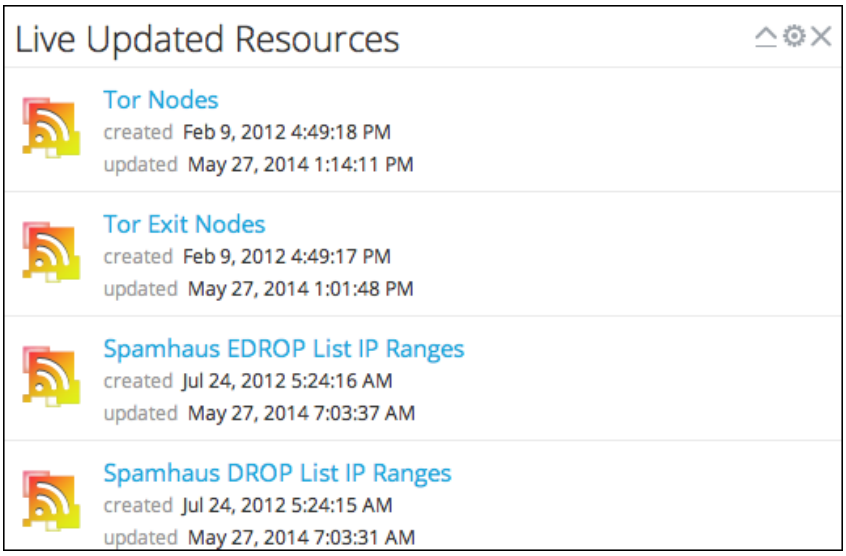
The grid is a subset of the subscriptions grid in the Live Manage View.

Value	Description
Name	Displays the name of the subscription.
Type	Specifies the type of subscription.
Description	Describes the type of information supplied by the subscription.

Live Updated Resources Dashlet

The Live Updated Resources dashlet displays a list of Live CMS resources that are tagged as updated for the configured Content Management System (CMS) server. You can click on the resource title to go to a detailed view of the resource.

To display this dashlet in the Security Analytics dashboard or as part of a custom dashboard, click  > **Add Dashlet** in the dashboard toolbar and select **Live Updated Resources**.



Features

This dashlet has a paged view of updated Live resources and provides the following information about each resource.

This dashlet has a page view of featured Live resources and provides the following information about each resource.

Value	Description
 Resource Type Icon	Each type of Live resource is represented by an icon. For example, the icon in the screen capture represents a Decoder feed. Clicking the **Resource Type** icon opens a new browser tab with the detailed view of the resource in the Live Resource view.

Value	Description
Resource Name	The name of the resource, for example, **Spamhaus EDROP List IP Ranges**. Clicking the Resource Name displays the detailed view of the resource in the Live Resource view. The view opens in the current browser tab.
Date Created	The date the resource was created.
Last Updated Date	The date the resource was last updated.

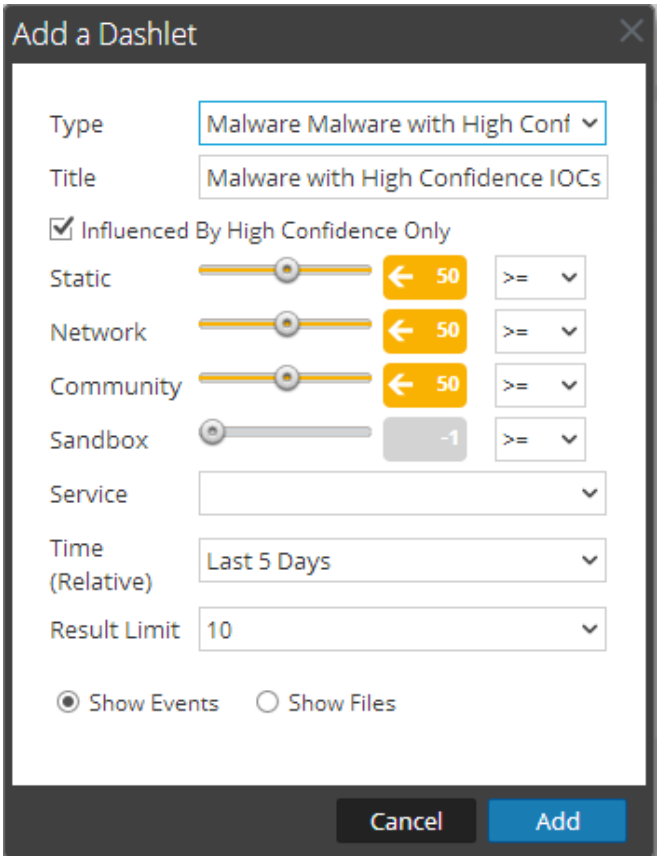
Malware Malware with High Confidence IOCs and High Scores Dashlet

The Malware Malware with High Confidence IOCs and High Scores dashlet presents the events that Malware Analysis detected with Indicators of Compromise, high likelihood of harboring malware, and high scores in the scoring modules. This dashlet is available in the Unified dashboard and in the Malware view. When a Malware Analyst first logs on to Security Analytics, by default the only visible dashlet in the Unified view is the What's New dashlet. The analyst must create any additional Malware dashlets.

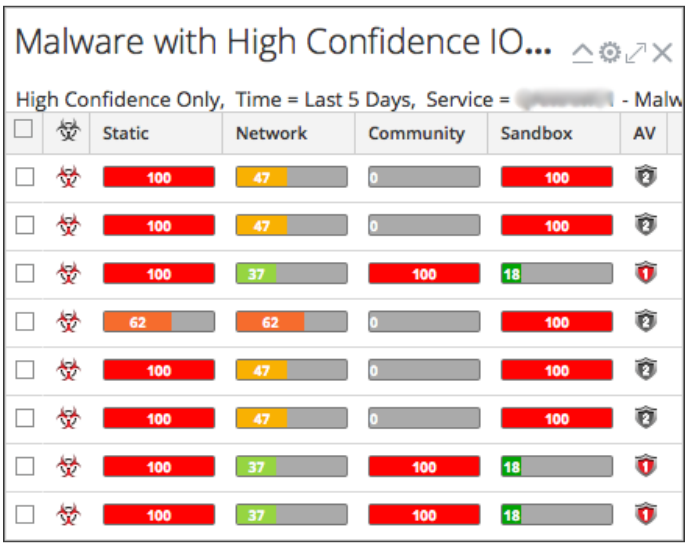
The Malware Malware with High Confidence IOCs and High Scores dashlet is configurable. You can create multiple copies of the dashlet, filter results, and configure the display of results as an Events List or a Files List.

To display this dashlet in the **Security Analytics Dashboard** or as part of a custom dashboard, click  > **Add Dashlet** in the dashboard toolbar and select **Malware Malware with High Confidence IOCs and High Scores** from the **Type** drop-down menu.

This is an example of the Malware Malware with High Confidence IOCs and High Scores dashlet settings.



This is an example of the Malware Malware with High Confidence IOCs and High Scores dashlet.



Features

The following table lists configurable values for this dashlet.

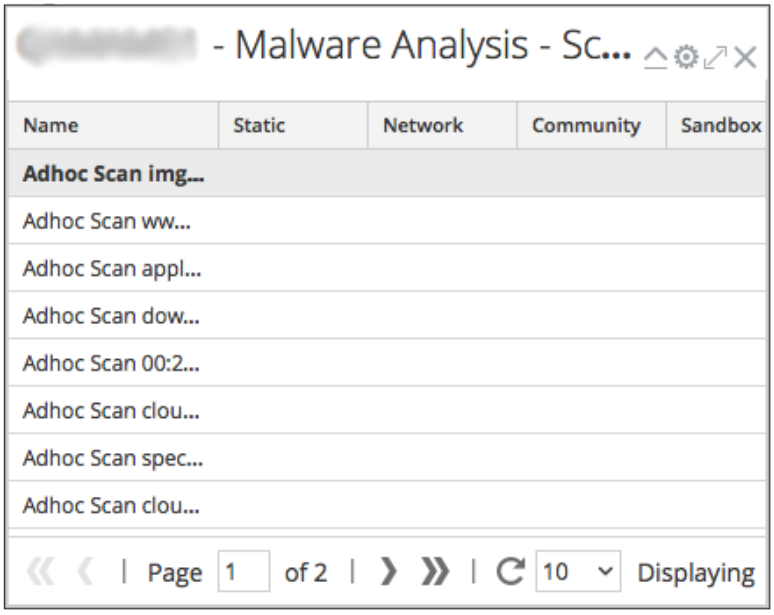
Variable	Description
Title	Identifies the name of the dashlet. Each dashlet needs a unique name, especially if you have more than one instance of the same dashlet. The name appears in the title bar of the dashlet.
Influenced by High Confidence Only	When checked, only events and files that were flagged as High Confidence (or likelihood) for containing Indicators of Compromise are displayed in the dashlet.
Static, Network, Community, Sandbox	Filters the results based on the scores for each scoring module. You can set the value as =, <=, or >=.
Result Limit	Sets the number of results to be displayed. Possible values in the drop-down list are 5, 10, 20, 30, or 40.
Service	Selects the service to be monitored.

Variable	Description
Time (Relative)	Limits the time range of displayed results.
Show Events or Show Files	Specifies the form of the results, either Events List or Files List format.

Malware Scan Jobs List Dashlet

The Malware Scan Jobs List dashlet displays the same Scan Jobs List found in the Select a Malware Service dialog. You can open completed scans directly from this dashlet.

To display this dashlet in the Security Analytics dashboard or as part of a custom dashboard, click  > **Add Dashlet** in the dashboard toolbar and select **Malware Scan Jobs List**.



Features

The columns in this Scan Jobs list are the same as those in the Scan Jobs List in the Select a Malware Service dialog.

Double-clicking on a job allows you to view a job in the Investigation > Malware Analysis view. The Summary of Events for the selected scan opens with the default dashlets displayed in a new browser tab.

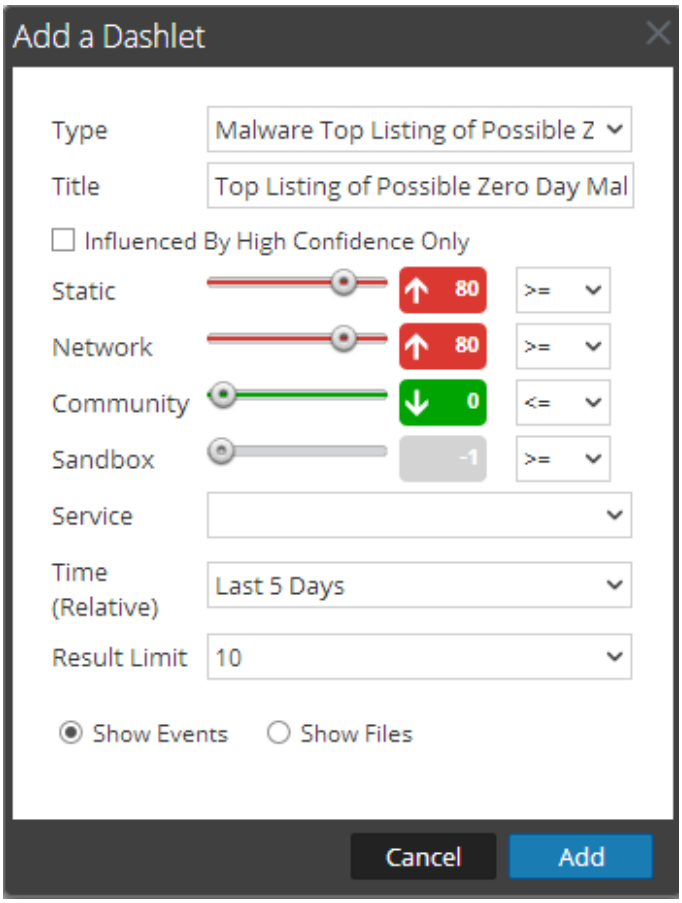
Malware Top Listing of Possible Zero Day Malware Dashlet

The Top Listing of Possible Zero Day Malware dashlet presents the top 10 events indicative of a possible zero day attack in the Malware Analysis Events List or the Files List. This dashlet is available in the dashboard and in the Malware view. When a Malware Analyst first logs in to Security Analytics, by default the only visible dashlet in the view is the What's New dashlet. The analyst must create any additional Malware dashlets.

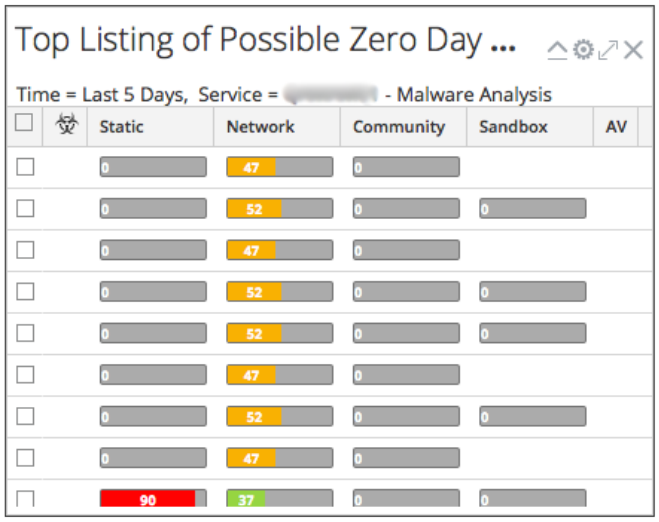
The Top Listing of Possible Zero Day Malware dashlet is configurable. You can create multiple copies of the dashlet, filter results, and configure the display of results as an Events List or a Files List. From this dashlet, you can launch an Malware Analysis investigation of an event directly by double-clicking the event; you do not have to go to the Investigation > Malware view to begin.

To display this dashlet in the **Security Analytics** dashboard or as part of a custom dashboard, click  > **Add Dashlet** in the dashboard toolbar and select **Malware Top Listing of Possible Zero Day Malware** from the **Type** drop-down menu.

This is an example of the dashlet settings configured to display the Events List.



This is an example of the dashlet. The features in the dashlet are the same as those on the Malware Analysis Events List or the Files List.



Features

The following table lists configurable values for this dashlet.

Variable	Description
Title	Identifies the name of the dashlet. Each dashlet needs a unique name, especially if you have more than one instance of the same dashlet. The name appears in the title bar of the dashlet.
Influenced by High Confidence Only	When checked, only events and files that were flagged as High Confidence (or likelihood) for containing Indicators of Compromise are displayed in the dashlet.
Static, Network, Community, Sandbox	Filters the results based on the scores for each scoring module. You can set the value as =, <=, or >=. The operator for the community filter is less than or equal to the applied slider value by default. The operator for the other filters is greater than or equal to by default.
Service	Selects the service to be monitored.

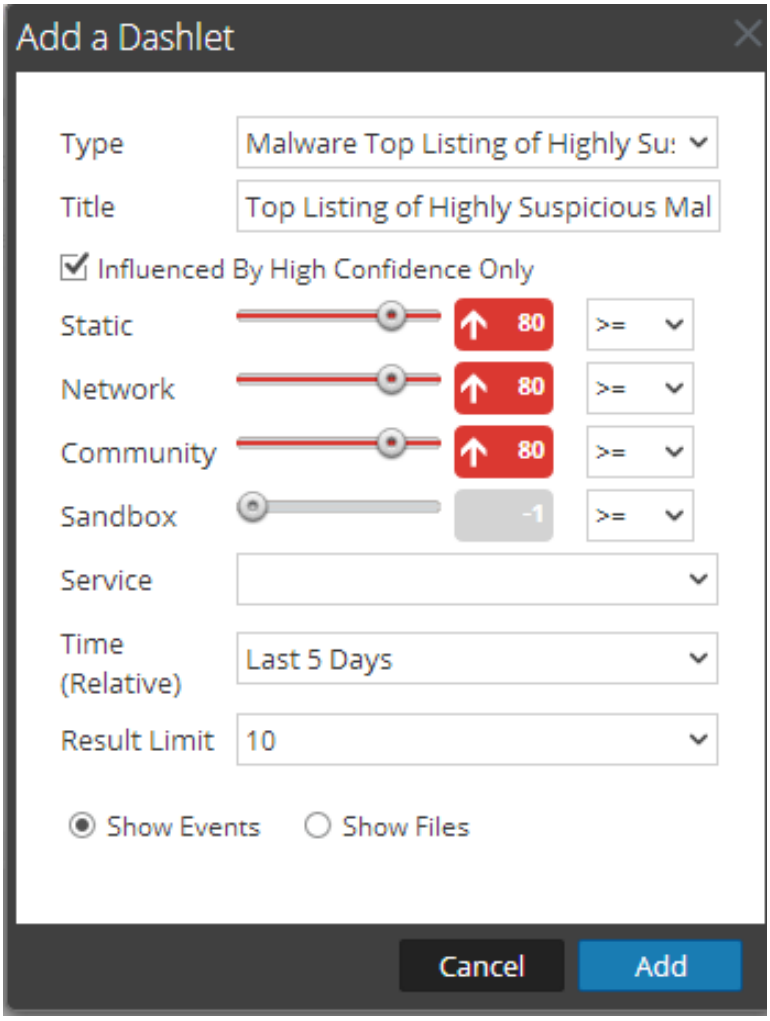
Variable	Description
Time (Relative)	Limits the time range of displayed results.
Result Limit	Sets the number of results to be displayed. Possible values in the drop-down list are 5, 10, 20, 30, or 40.
Show Events or Show Files	Specifies the form of the results, either Events List or Files List format.

Malware Top Listing of Highly Suspicious Malware Dashlet

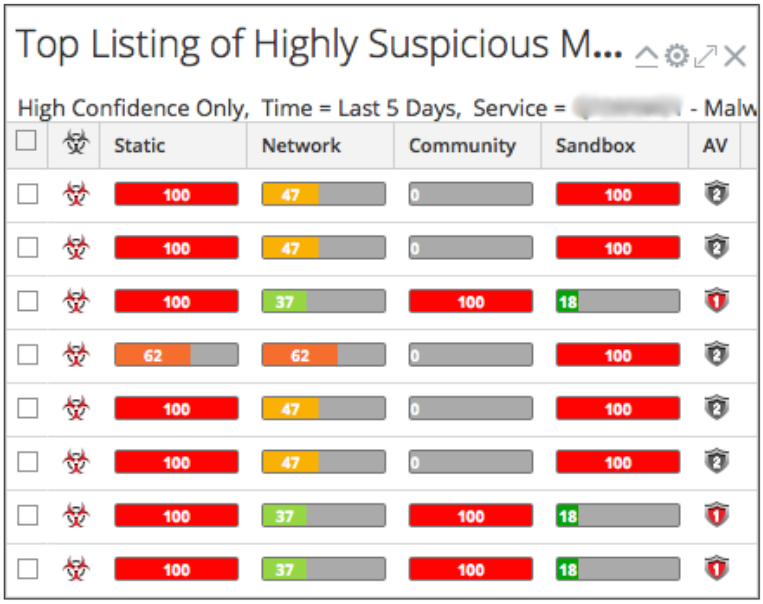
The Malware Top Listing of Highly Suspicious Malware dashlet presents the top 10 most suspicious events in the Malware Analysis Events List or the Files List. This dashlet is available in the dashboard and in the Malware Analysis view. When a Malware Analyst first logs in to Security Analytics, by default the only visible dashlet dashboard is the What's New dashlet. The analyst must create any additional Malware Analysis dashlets.

The Malware Top Listing of Highly Suspicious Malware dashlet is configurable. You can create multiple copies of the dashlet, filter results, and configure the display of results as an Events List or a Files List.

To display this dashlet in the **Security Analytics Dashboard** or as part of a custom dashboard, click > **Add Dashlet** in the dashboard toolbar and select **Malware Top Listing of Highly Suspicious Malware** from the **Type** drop-down menu.



This is an example of the dashlet.



Features

The features are the same as the features of the **Malware Analysis Events List and Files List** (see the *Investigation and Malware Analysis Guide* for details). To launch a Malware Analysis investigation of an item in the dashlet, double-click an event or file name in the grid.

The following table lists configurable values for this dashlet.

Variable	Description
Title	Identifies the name of the dashlet. Each dashlet needs a unique name, especially if you have more than one instance of the same dashlet. The name appears in the title bar of the dashlet.
Influenced by High Confidence Only	When checked, only events and files that were flagged as High Confidence (or likelihood) for containing Indicators of Compromise are displayed in the dashlet.
Static, Network, Community, Sandbox	Filters the results based on the scores for each scoring module. You can set the value as =, <=, or >=.
Service	Selects the service to be monitored.

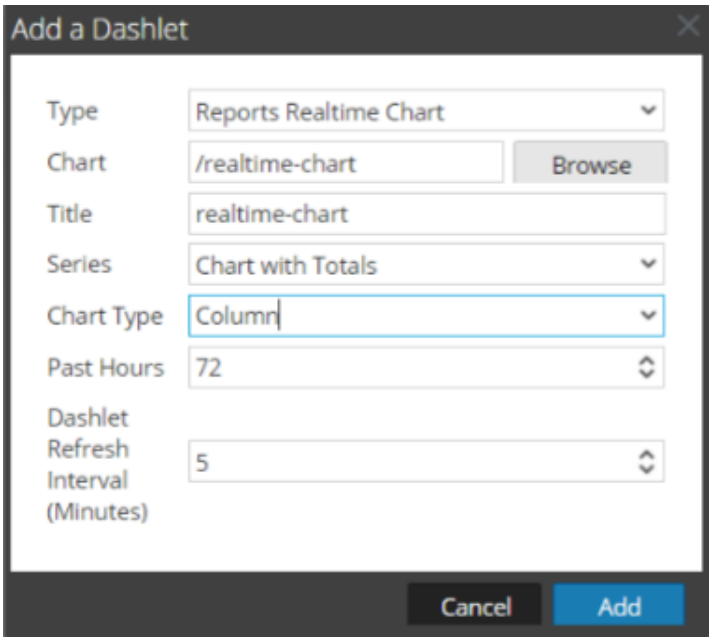
Variable	Description
Time (Relative)	Limits the time range of displayed results.
Result Limit	Sets the number of results to be displayed. Possible values in the drop-down list are 5, 10, 20, 30, or 40.
Show Events or Show Files	Specifies the form of the results, either Events List or Files List format.

Reports Realtime Chart Dashlet

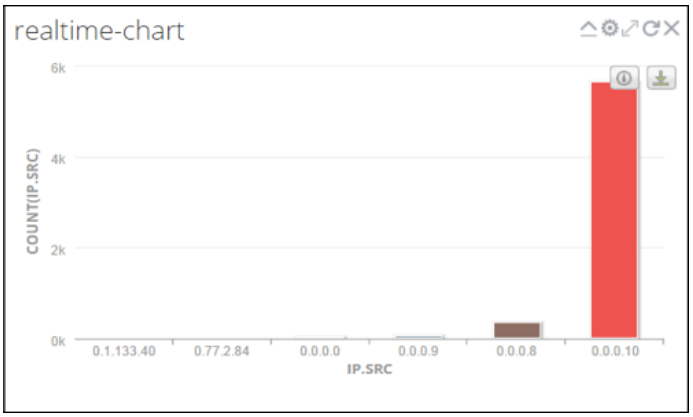
The Reports Realtime Chart dashlet displays one of the charts from the list of charts that you defined. The chart output is from the live data and it refreshes itself based on the refresh interval that you set. Each chart is defined by the Chart Type and Past Hours value that you select.

You can select either the Chart Values over Time or Chart with Totals option. The chart graphs the current data and does not display data points for historical data.

The chart is generated for data depending on the time interval that you defined in the chart definition. The data are available from a maximum of the past 20 time intervals. For example, if in the chart definition you selected a refresh interval as five minutes and past hour as one hour, the chart displays data from the past 60 minutes. The chart in the dashlet refreshes itself based on the dashlet refresh interval that you have defined. In the **Past Hours** field, you can select values between 1 to 72 hours. The default value is **24** hours.



To display this dashlet in the **Security Analytics** dashboard or as part of a custom dashboard, click > **Add Dashlet** in the dashboard toolbar and select the **Reports Realtime Chart** from the **Type** drop-down menu.



Features

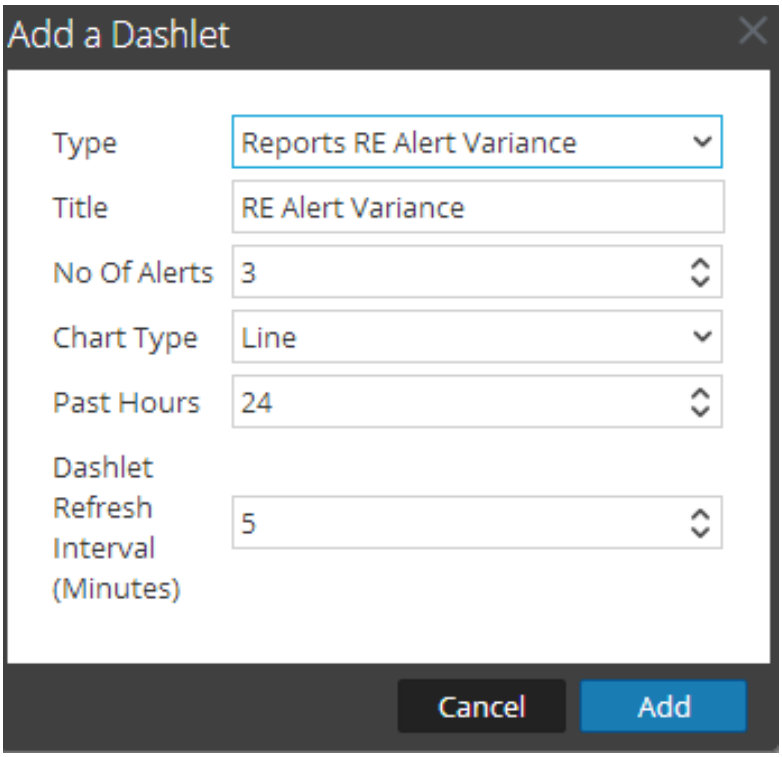
Chart options are listed in the following table.

Variable	Description
Chart	Select a chart from the already defined charts. You can select only one chart per dashlet.
Title	Type a name for the Reporting Realtime Chart dashlet. The name appears in the title bar of the dashlet.
Series	**Chart Values over Time**: The chart displays the change in values for the selected time.
	Chart with Totals: The chart displays a total for each aggregate value for the selected time.
Chart Type	Select the type of chart that you want in the dashlet. The values provided in the drop-down are: bar, column, and line.
Past Hours	Select the past time interval.
Dashlet Refresh Interval (Minutes)	Set the time interval in minutes at which the data in the dashlet gets refreshed. The interval value ranges from 1-180 minutes.

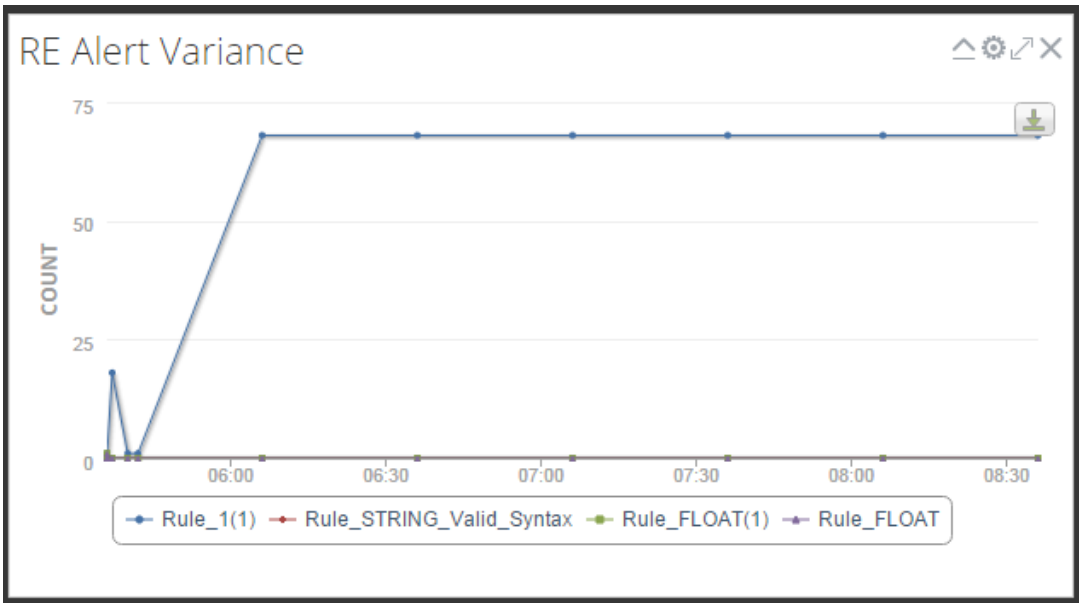
Reports RE Alert Variance Dashlet

The Reports RE Alert Variance dashlet is a configurable dashlet that depicts top alerts in four different time series chart types. You can configure the results to include in the chart (from the top 2 alerts to the top 15 alerts in the specified time range).

To display this dashlet in the **Security Analytics** dashboard or as part of a custom dashboard, select  > **Add Dashlet** in the dashboard toolbar and select **Reports RE Alert Variance** from the **Type** drop-down menu.



The following figure is an example:



Features

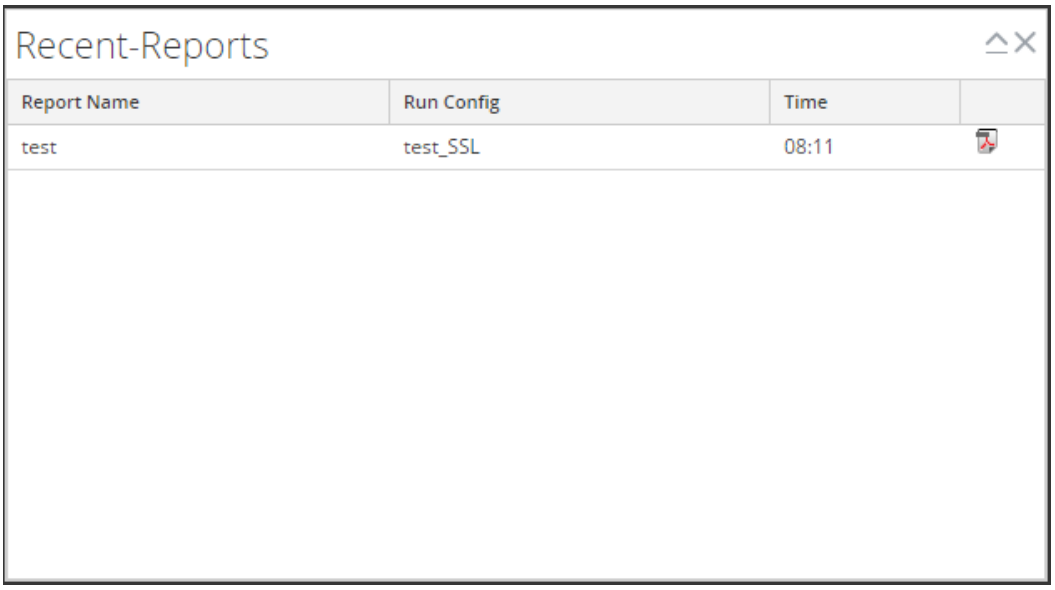
This dashlet is a visual representation of the alerts most frequently triggered by the associated Reporting Engine. Each chart type can be defined by the number of alerts and past hours from when the alerts need to be fetched, and the dashlet refresh interval for the chart to be refreshed.

Variable	Description
Title	Provide a name for the Reporter Realtime Chart dashlet. The name appears in the title bar of the dashlet.
No of Alerts	Select the number of alerts to be considered while configuring the dashlet. The value ranges from 2 - 15.
Chart Type	Select the type of chart that you want in the dashlet: • Bar (X-axis = Count and Y-axis = Alert name) • Column (X-axis = Count and Y-axis = Alert name) • Line (X-axis = Count and Y-axis = Alert name)
Past Hours	Select the time from when the alerts need to be fetched.
Dashlet Refresh Interval (Minutes)	Set the time interval in minutes at which the data in the dashlet gets refreshed. The interval value ranges from 1-180 minutes.

Reports Recent Run Report Dashlet

The Reports Recent Run Report dashlet consists of a list of reports that were run recently in Security Analytics. The recent reports displayed are from the last 24 hours.

To display this dashlet in the Security Analytics dashboard or as part of a custom dashboard, click > **Add Dashlet** in the dashboard toolbar and select **Reports Recent Run Report** from the **Type** drop-down.



Features

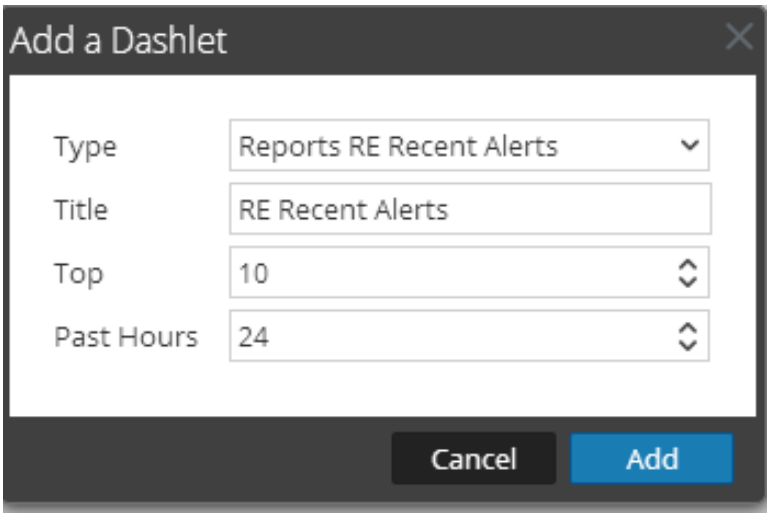
The columns present in the dashlet by default are described in the following table.

Column	Description
Report Name	The name of the recently run report.
Run Config	The run configuration of the recently run report.
Time	The time the report was scheduled.
Export	Click on the export icon ( ) to export the file.

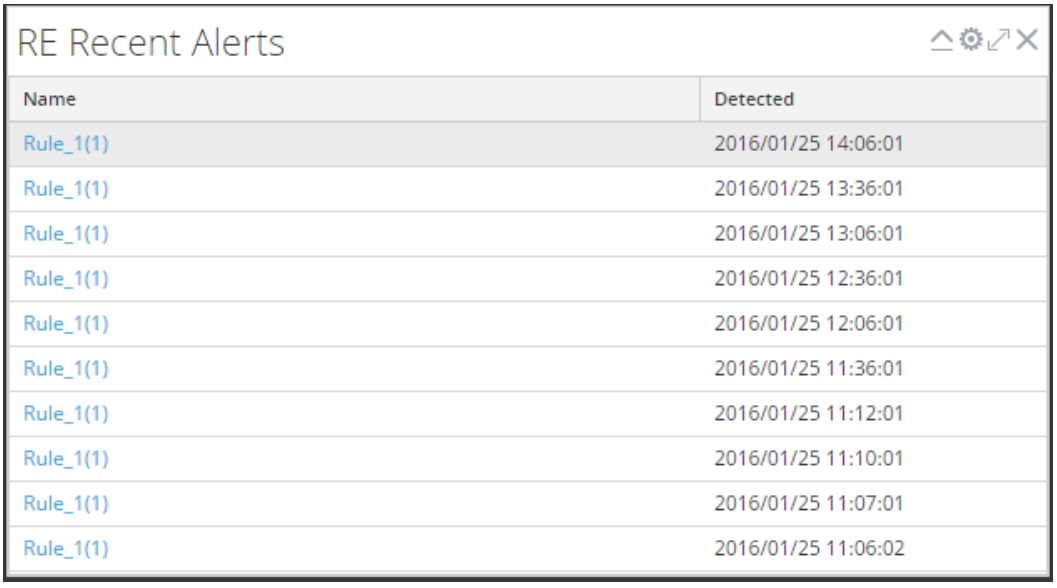
Reports RE Recent Alerts Dashlet

The Reports RE Recent Alerts dashlet displays the latest alerts on the dashboard. You can configure the number of latest alerts to be displayed and also specify the time range from when the alerts needs to be fetched.

To display this dashlet in the Security Analytics dashboard or as part of a custom dashboard, click  > **Add Dashlet** in the dashboard toolbar and select **Reports RE Recent Alerts** from the **Type** drop-down menu.



The following figure is an example:



Features

The following table describes the columns in the Reports RE Recent Alerts dashlet.

Column	Description
Name	The name of the alert as defined.
Detected	The date and time that the alert fired. This detection time is when Security Analytics detected the conditions for firing this alert.

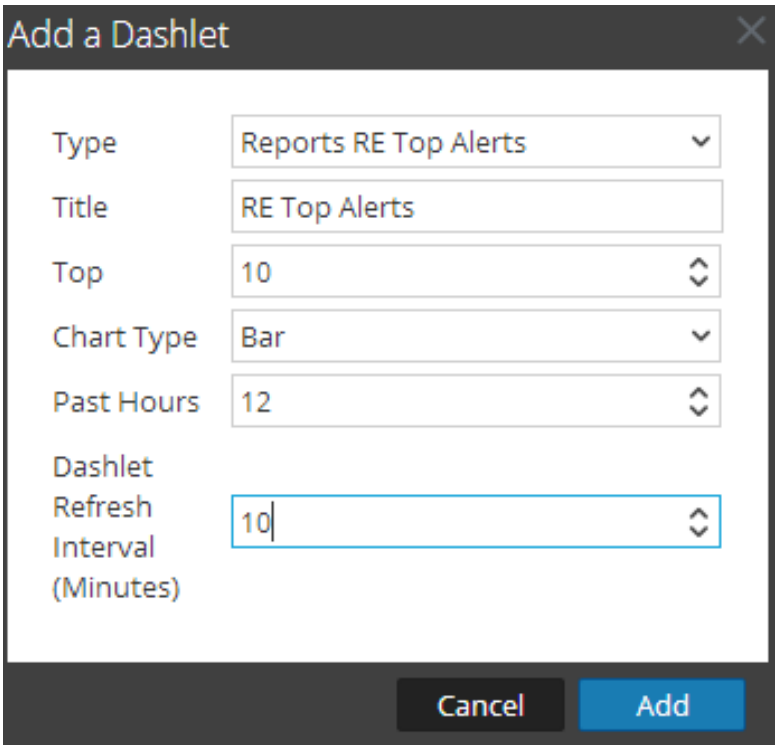
Reporting RE Top Alerts Dashlet

The Reports RE Top Alerts dashlet is a configurable dashlet that depicts top alerts in four chart types. You can configure the results to include in the chart (from the top 2 alerts to the top 15 alerts in the specified time range).

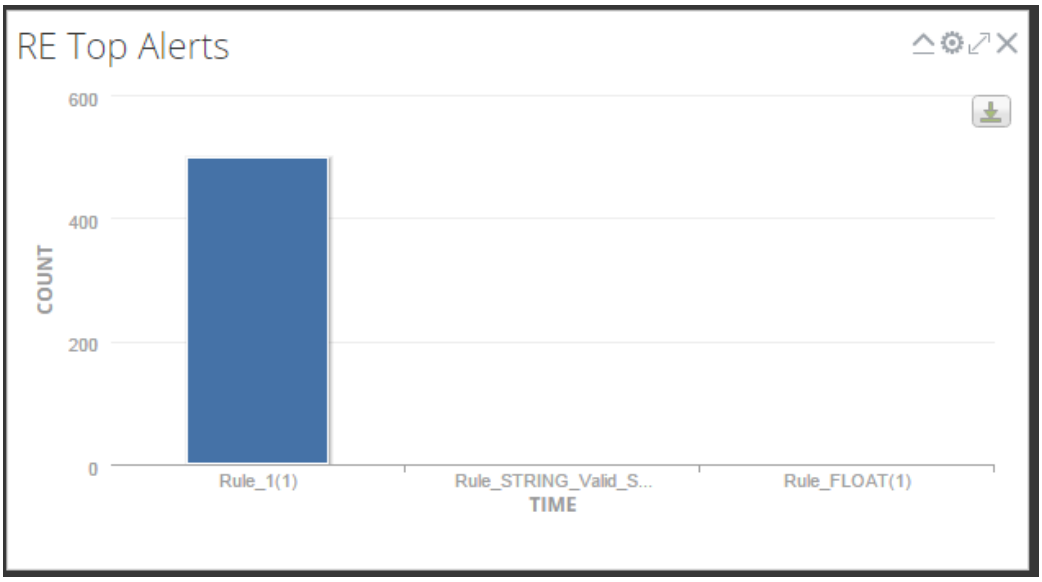
The chart is summarized for each top alert against the number of events triggered by the alert for the defined time and refresh intervals. The first data point in the chart defines the number of events (alert count) triggered by the alert for the defined time. The subsequent data points are depicted by adding the alert count in the first data point and alert count in the defined refresh intervals.

For example, if for the defined time range, the number of events (alert count) triggered by the alert is 10, then the first data point in the chart is shown as 10. The subsequent data point = 10 + number of events (alert count) triggered by the alert in the defined dashlet refresh interval.

To display this dashlet in the Security Analytics dashboard or as part of a custom dashboard, click  > **Add Dashlet** in the dashboard toolbar and select **Reports RE Top Alerts** from the **Type** drop-down menu.



The following figure is an example:



Features

This dashlet is a visual representation of the alerts most frequently triggered by the associated Reporting Engine. Each chart type can be defined by the number of top alerts, the time from when the alerts needs to be fetched, and the dashlet refresh interval for the chart to be refreshed.

Variable	Description
Chart Type	Select the type of chart that you want in the dashlet: • Bar (X-axis = Count and Y-axis = Alert name) • Column (X-axis = Count and Y-axis = Alert name) • Pie • Line (X-axis = Count and Y-axis = Alert name) • Tabular (X-axis = Count and Y-axis = Alert name)
Title	Type a name for the Reporting Realtime Chart dashlet. The name appears in the title bar of the dashlet.
Top	Select the number of top alerts to be considered while configuring the dashlet. The value ranges from 2 - 15.
Past Hours	Select the time from when the alerts need to be fetched.

Variable	Description
Dashlet Refresh Interval (Minutes)	Set the time interval in minutes at which the data in the dashlet gets refreshed. The interval value ranges from 1-180 minutes.