IntroSpect 2.4

a Hewlett Packard
Enterprise company

User Guide

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
6280 America Center Drive
San Jose, CA 95002
USA

Contents

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision History	Date	Change Description
Revision 1	October 2, 2018	IntroSpect 2.4 release. Includes Analytics and Configuration updates.
Revision 2	February 15, 2019	Added the System Status chapter.
Revision 3	April 3, 2019	Added the following: ■ Procedure for Adding Periodic Alarm Notifications (**Menu > Configuration > System > Alarms Email**). ■ Tab details for the **Global Configuration** tab (**Menu > Analytics > Global Configuration**).

Contacting Support

Table 2: *Contact Information*

Main Site	www.arubanetworks.com
Support	hpe-aruba-introspect-support@hpe.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	hpe.com/networking/support
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: sirt@arubanetworks.com

IntroSpect's behavioral analytics platform automates the detection of attacks and risky behaviors inside an organization and boosts the power of security teams by accelerating alert prioritization, incident investigation and threat-hunting efforts.

IntroSpect ingests logs from the security infrastructure (such as Active Directory, firewall, web proxy, VPN, DLP, IDS, DNS) and combines them with network flows and packets. Then IntroSpect applies behavioral analytics models across multiple dimensions: authentication, access to high value resources, exfiltration, remote access, cloud application usage, Internet activity and physical access.

The broad range of data sources and behavioral models enables IntroSpect to create comprehensive, high fidelity Entity360 risk profiles for users and hosts. Unsupervised Machine Learning (ML) models establish behavioral baselines and flag unusual activity. This is combined with supervised ML models and adaptive techniques to reliably link anomalous and malicious activity, and reduce false positives. IntroSpect combines the results of its analytics modules with integrated forensics, eliminating context-switching for investigations and making threat detection and alert investigation easy.

About This Guide

This guide provides an overview of the features and functions of the Aruba IntroSpect Analyzer application and describes the basic tasks users can perform from the user interface (UI).

The document Revision History lists details of edits to each revision.

Common Features

Some features are common to many areas of the application, and work in the same way wherever they appear. These features are documented in this section.

Icons

Each entity or node type is displayed with a specific icon throughout the system, so that you can easily see the type.

Destination IP Addresses display the icon but are not entities in the system. Also, some nodes may not appear as entities until they have been evaluated.

Icon	Type
	User
	Host
	IP Address
	Watchlist

Risk Score Colors

Colors indicate risk score categories, so that you can see at a glance the quantity of a risk group, and the details for specific entities.

Color	Risk Score
	High Risk
	Medium Risk
	Low Risk
	Very Low Risk

Required Fields

Required fields are marked with an asterisk * when filling out forms.

NOTE

Administrator privileges are required to complete the following steps.

Sort by Column Headers

Many columns in the Analyzer web UI are sortable. You can also drag the edges of a column to change its size.

- To sort by a column, click on a column header that displays arrows .

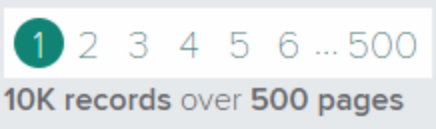
NOTE

When you sort the table by a column, the header display for that column changes to a single arrow . You can then toggle the sort order for that column. Click on a different column to sort the table by that column.

- To toggle the sort order for a column, click on the single arrow .

Pagination

Use the pagination controls to navigate through pages of your results. The count of results displayed and total shows below the page links (10K records over 500 pages in the example).



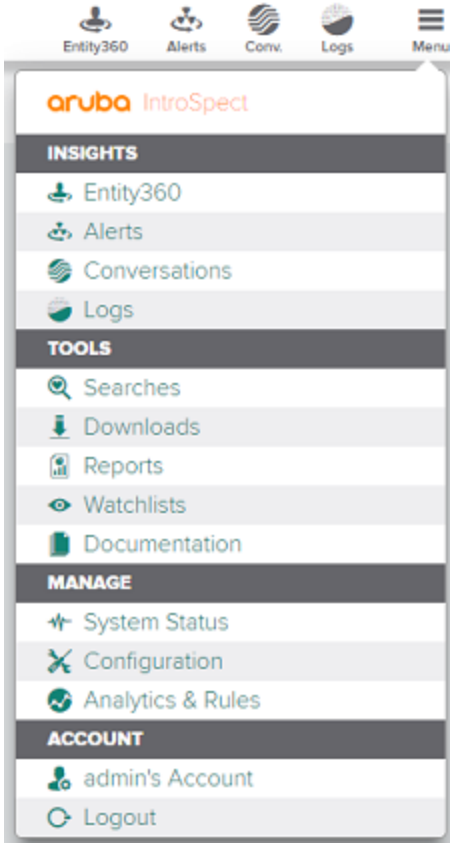
The number of results to show on a page is displayed in the **settings** dropdown list (20 in the example).

Navigating in IntroSpect

Use the top navigation menu to access different parts of IntroSpect [[[Undefined variable General.Product]]].

Click the icons to go to the corresponding sections. Use the menu to navigate to additional options.

Figure 1 *Navigation Menu*



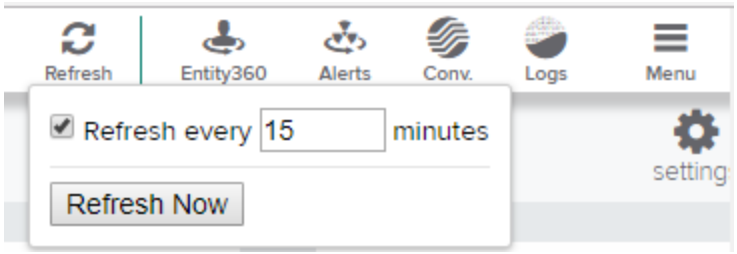
A yellow counter displays if you have downloads available.

Some pages have an option to set the data to refresh at a specified interval. Click the **Refresh** icon to access these options.

Setting a Refresh Interval

To set a refresh interval, check the **Refresh** box and set an interval, in minutes. You can also click **Refresh Now** to update the data immediately.

Figure 2 *Refresh Interval*



Using Filters

You can filter the information you see, and create and save searches for reuse. The filters on the left panel of many pages can be used to select groups of data. Apply filters to enter them as search queries in the search bar. You can then continue to edit them using additional criteria, and save the search to be used later.

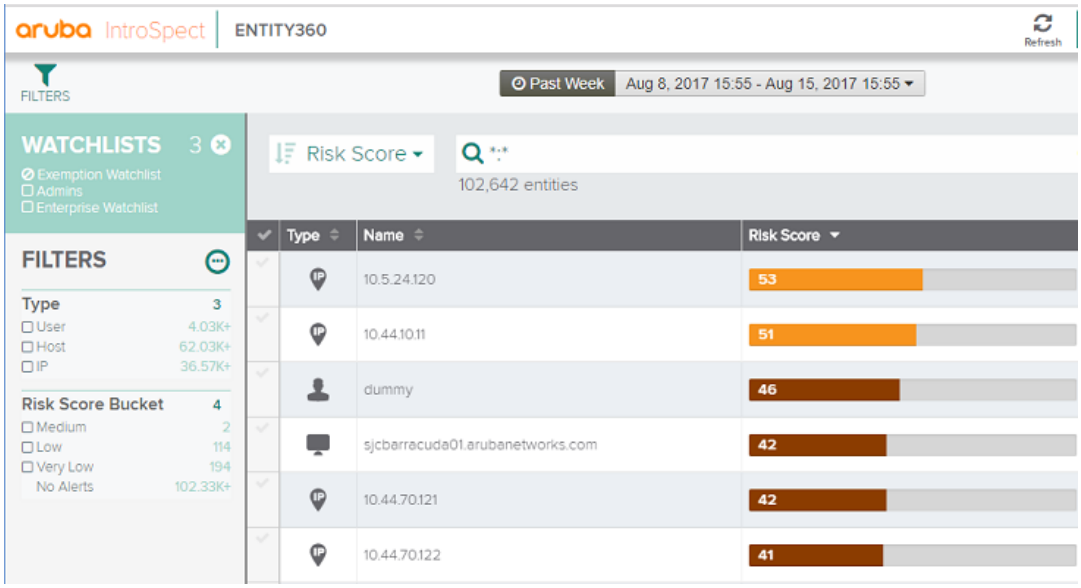
For pages with more filter options, there is an additional option to select from a list of filters and reorder your filters. See Selecting Filters for more information.

Use filters to narrow what is displayed on the screen. The filters appear in a panel on the left side of some screens. When you make selections, the results display is updated immediately.

NOTE

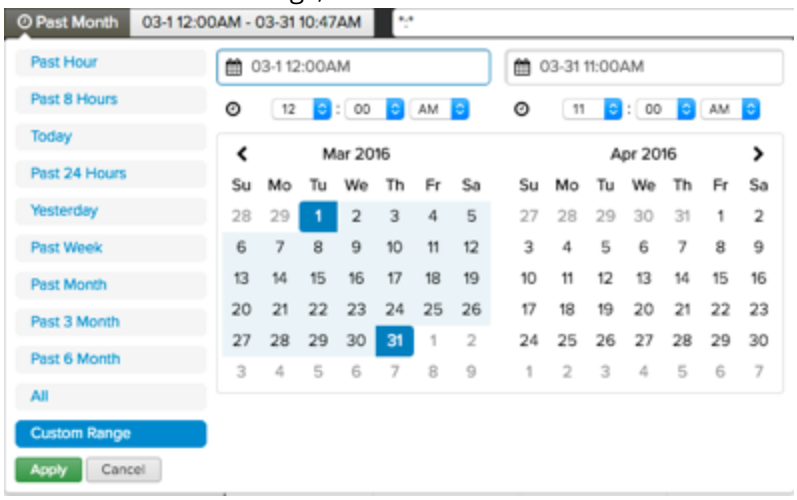
When you select a date range or time span on any page, that selection will be applied on all pages as you view data on other pages, until you change the selection.

Table 3: *Filter Options*



Filtering options

- To select a new date range, click the date bar to access the menu and make a selection.



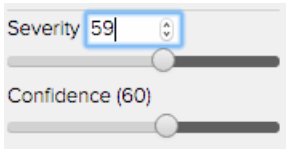
- To filter by watchlist, select one or more watchlists. See View Watchlists for more information.
- To show or hide the filters panel, click the » or « icon.
- To select filters, check one or more boxes for the criteria you want to see.
- To select values, click the header or count for a group to open Selecting Values and modify the values.
- To apply filters as a search query, click to enter your selected filters in the Search field as a search query, and to use the search functions for the query.

Filter by Severity and Confidence

Use the severity and confidence on some filters and charts to filter what is displayed by these criteria.

To change severity or confidence:

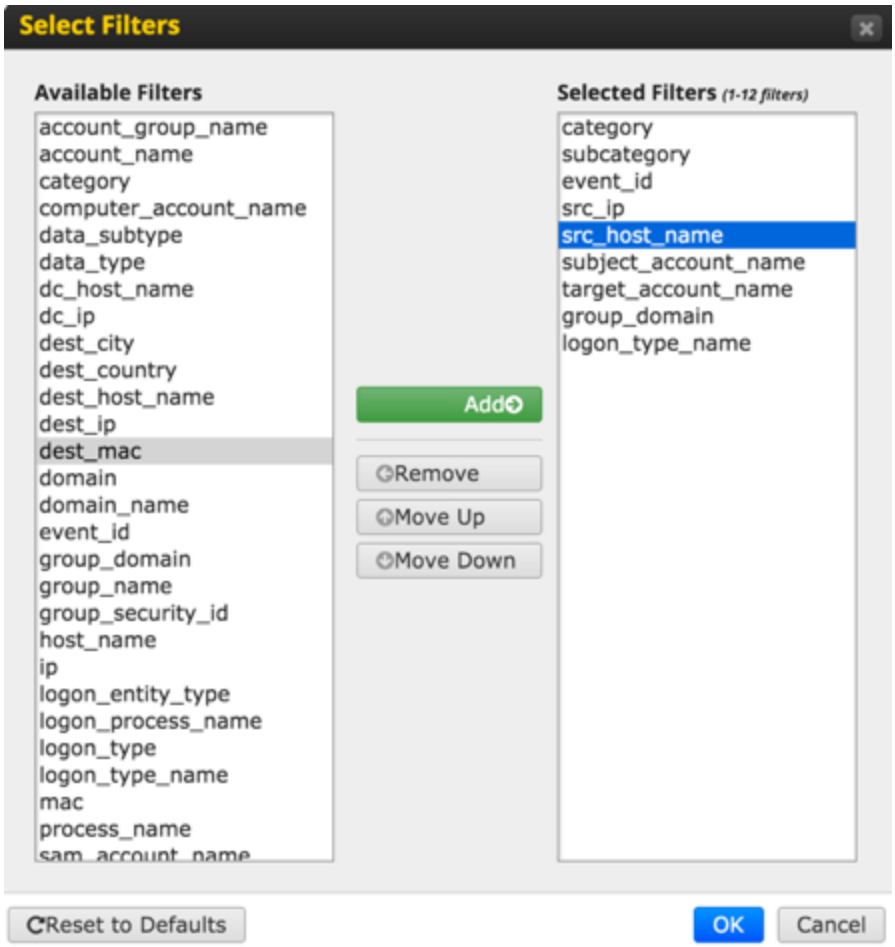
1. Drag to increase or decrease the levels and filter your results accordingly.
2. Click on the word or number to enter a specific value.



Selecting Filters

For pages with more filter options, there is an additional option to select from a list of filters and reorder your filters.

- To access **Select Filters**, click at the top of the filters panel.
- To add a filter, select an option from the left and click **Add**.
- To remove a filter, select an option from the right and click **Remove**.
- To reorder a filter, select an option from the right and click **Move Up** or **Move Down**.
- To reset to the default filters, click **Reset to Defaults**.

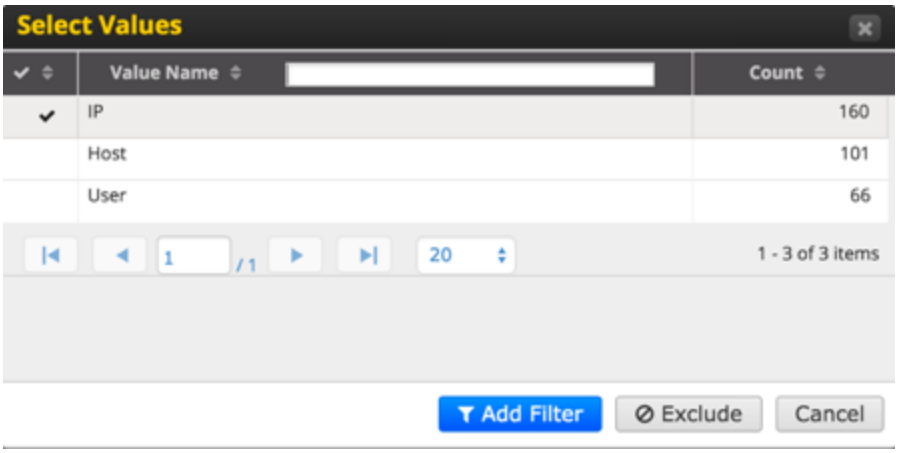


Selecting Values

You can select objects in a group to use in your filter. Only the objects in that group appear in the list, as opposed to using the Edit button to see all available filters. See Selecting Filters for those options.

To specify values for a filter group:

1. From the Using Filters pane, click on the header or count 3 icon for a group.
2. Select one or more filters you want to include, or enter text to search for values in the list. When you select a filter, the count of results displays on the right as you type.
3. Choose an option to modify your filter by clicking one of the buttons:
   - **Add Filter**, to add the specified values to your filter.
   - **Exclude**, to exclude the specified values from your filter.
   - **Cancel**, to cancel the changes.



Using Search Features

Use the powerful search features in conjunction with Using Filters or on their own. Apply filters to enter them as search queries in the search bar. You can then continue to edit them using additional criteria, and save the search to be used later. You can also use the query language to enter search criteria directly.

Search results counts are displayed while the system is searching. When the search completes, the count is displayed in blue.

Search

Use Search functions to save, clear, or modify your filter selections, or to create new queries manually. You can also view the search documentation.

You can do the following from search:

- View the Search Documentation or searchable fields for a page.
- See your applied filters as a query.
- Manually enter or modify queries.
- Save a search.
- Clear all search criteria, including filters.

Viewing the Search Documentation

To view the search documentation, Click and select an option:

- Click the **Search Documentation** link to open the full document in a new page.
- Click an example link to add the query to your search.

Create or Edit a Query

To create or edit a query:

1. Start entering text for the field you want to use to see the valid entries. You can also enter a space to view all the valid fields.
2. Make a selection from the menu, or enter properly formatted queries manually.

- To perform the search, click **Search**.
- To save the search, click **Save** or click the **Actions** menu and select **Save query**.
- To clear the search and any filters, click **Clear**.

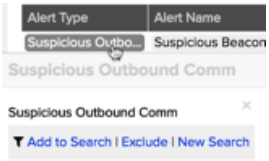
Search Using Fields

Click on fields in tables to add, exclude, or start a new search based on the field. This option is available from tables on many pages. When you make a selection, you will be taken to the relevant main page with the search criteria applied and displayed in the search field.

To modify the list search results:

1. Click **Add to Search** to search by this criteria.
2. Click **Exclude** to show everything except this criteria.
3. Click **New Search** to delete any existing searches or filters and initiate a search with only this criteria.

Figure 3 *Alert Search*



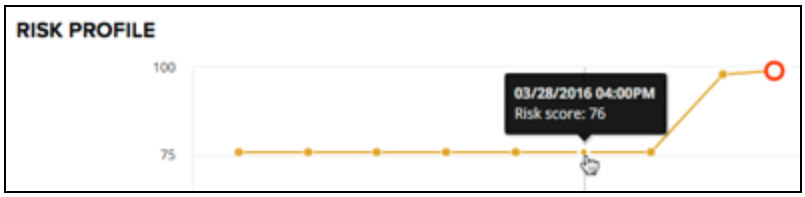
Using Charts

Some charts have common features that work in similar ways on different pages. Those are explained here.

View or Select Dates

When you hover on a chart, details for that point are displayed in a popup. Click and drag an area on the graph to select a different date range. Click Reset Zoom to reset the display to the full view.

Table 4: *Risk Profile*

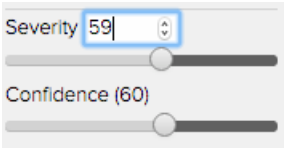


Filter by Severity and Confidence

Use the severity and confidence on some filters and charts to filter what is displayed by these criteria.

To change severity or confidence:

1. Drag to increase or decrease the levels and filter your results accordingly.
2. Click on the word or number to enter a specific value.



Viewing Graphs

Use graphs to see a graphical representation of your data and explore or drill down to different areas. Some graphs have common features that work in similar ways on different pages. Those are explained here.

Use the graph controls to zoom or move the display, or double-click an object on the graph to investigate the specific object.

Table 5: *Graph Controls*

Control	Description
	■ Click an arrow to move the entire graph. ■ Click the center button to center the graph.
	Click to toggle between the arrow and hand. ■ With the hand active, click on a node in the graph and drag to move that node. ■ With the arrow active, click outside the graph to drag it. If you click on a node, the behavior is the same as the hand.
	Click the + or - to zoom in or out incrementally. Drag the slider to the desired location to change dynamically.

Accessing Actions

The Actions menus (, , or) on some screens display options for performing common tasks in IntroSpect. There are common functions across many screens, but different options are available from E360, Alerts, Conversations, and Logs.

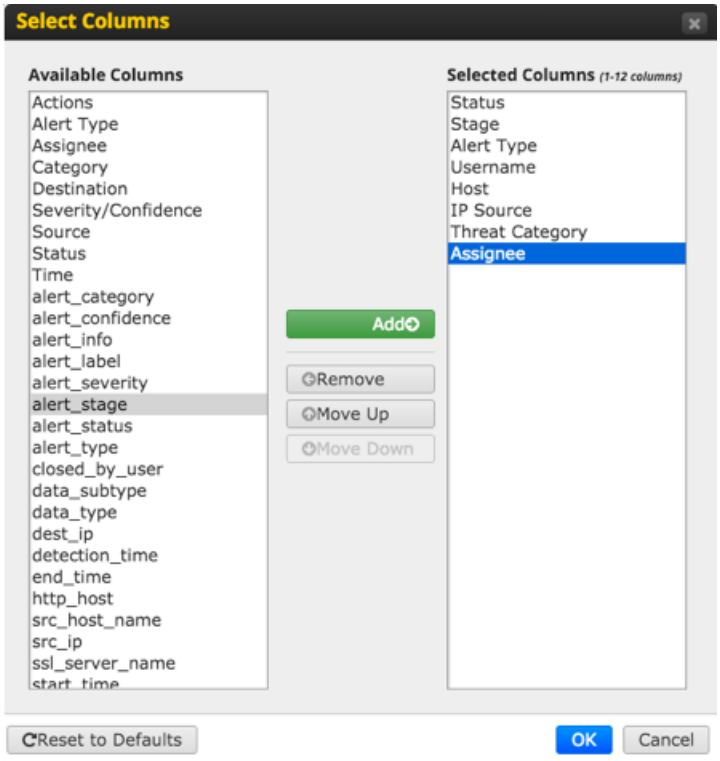
Export Data

Use the Export options to export some or all of your results to a file.

To export all visible data, choose **Export to CSV** or **Export to PDF** to export the results data to those formats.

Select Columns to Export

1. To select columns to export, choose **Select Column**.
2. In the **Select Columns** window, select and arrange the columns to export.
   - To add columns, select them from **Available Columns** and click **Add**.
   - To remove columns, select them from **Selected Columns** and click **Remove**.
   - To rearrange columns, select a column name from **Selected Columns** and click **Move Up** or **Move Down**



Create Rules

Use Rules to create custom alerts or modify IntroSpect 2.4 alerts based on saved searches or custom queries.

Access rules from the **Actions** menu on the following pages:

- **Alerts** page
- **Conversations** page .

You can create rules based on when conversations match your specified criteria, or when alerts match your criteria.

NOTE

If you choose **Create Rule** from the Alerts page or the Conversations page, any query displayed in the search field for that page will appear in the search field for your new rule. You can modify this, create a new query, or load a query from a saved search.

Use the **Severity** slider to change the severity required to trigger the alert. For conversation rules, you can also adjust the **Confidence** using the slider.

Modify Alerts Using Alert Rules

If you select **When alerts match:** for your rule, you can select an IntroSpect 2.4 alert name from the dropdown. When you view the **Alerts** page, the **Alert Name** column will display the type you select. You can sort by that column to group and more easily view alert types.

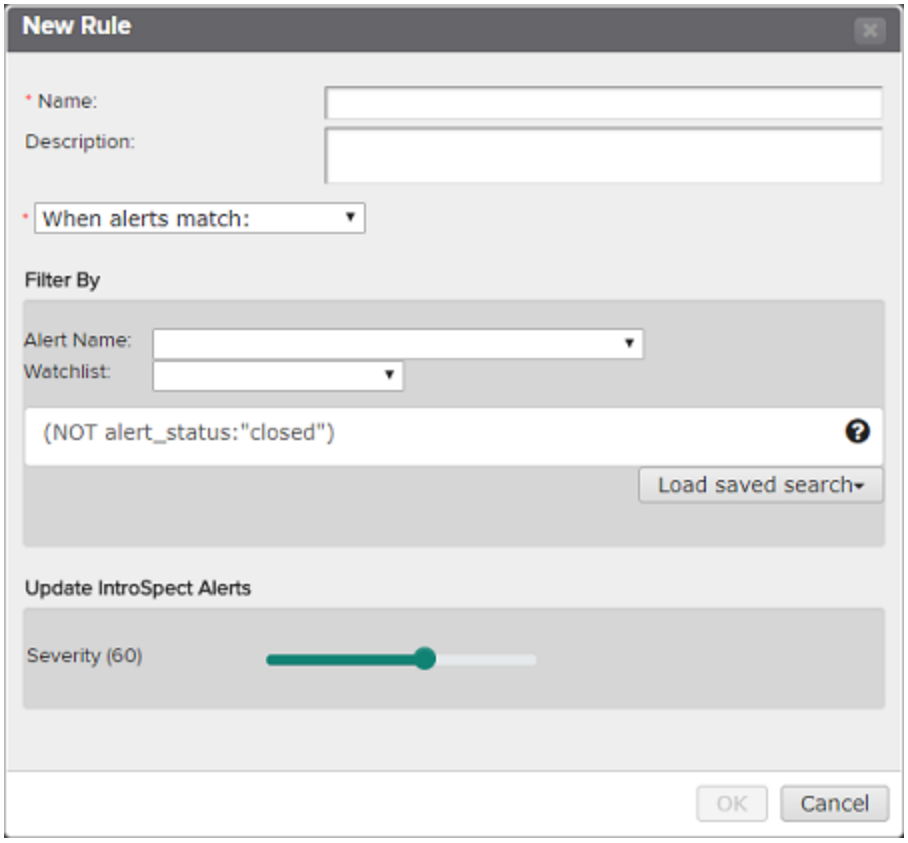
To create a new alert rule:

1. Enter a name for the rule.
2. Enter a description.
3. Select **When alerts match:** from the dropdown.
4. Select or enter an **Alert Name**.
5. Enter your search criteria, or click **Load saved search** and select a saved search.

NOTE

You must use the search fields or saved searches specific to the rule type you choose. If you choose **When alerts match:**, only use fields and saved searches valid for alerts. If you choose **When conversations match:**, only use fields and saved searches valid for conversations. Use the **Search** documentation to determine which fields are available.

6. Click **OK** to save the rule.



Create New Alerts Using Conversation Rules

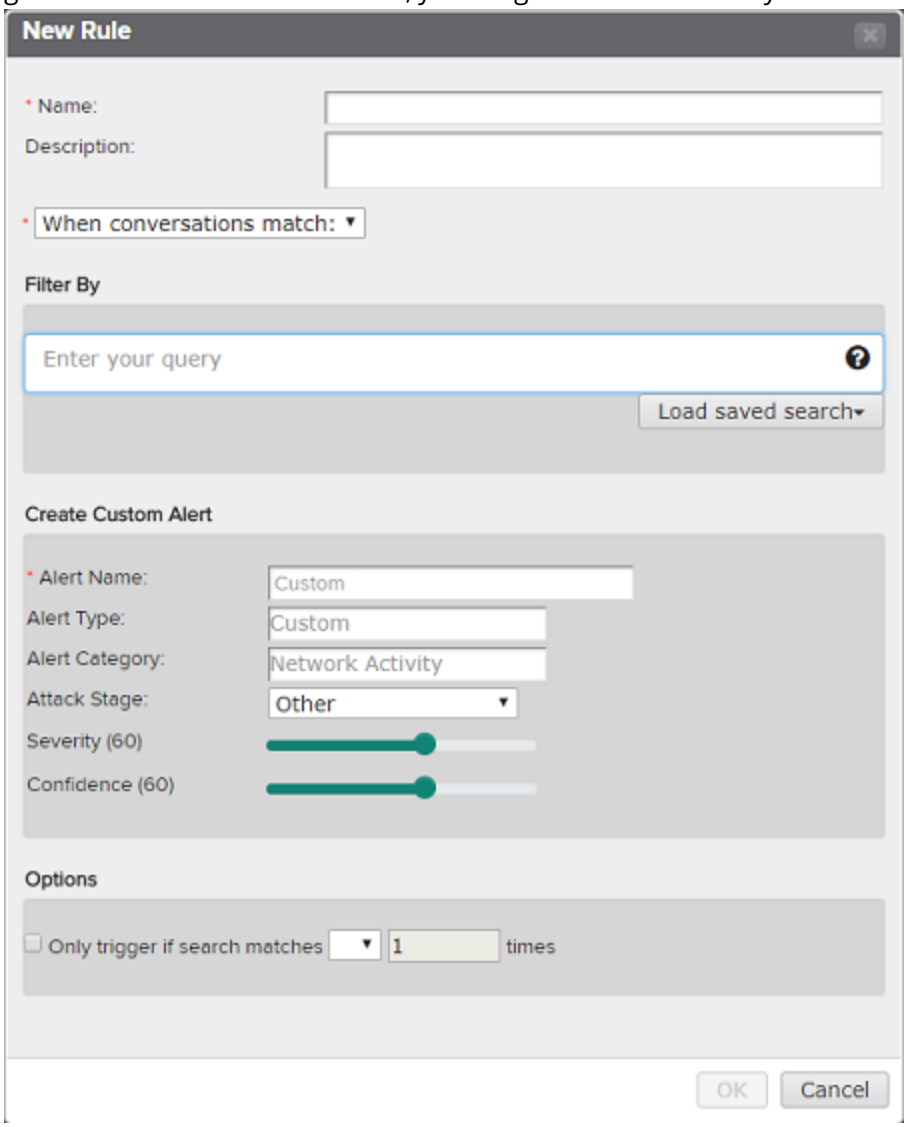
If you select **When conversations match** for your rule, you can select an **Attack Stage**, run the alert in trial mode rather than in production, and select the number of matches required to trigger the alert.

From the **Conversations** page , you can select the rule you created from the filters to see all alerts for that rule.

To create a conversation rule in the **New Rule** window:

1. Enter a **Name** for the rule.
2. Enter a **Description**.
3. Select **When conversations match:** from the dropdown.
4. Enter an alert name and search criteria, or click **Load saved search** and select a saved search.
5. In the **Create Custom Alert** section:
    a. Enter an **Alert Name** (required).
    b. Enter an **Alert Type** (optional).
    c. Enter an **Alert Category** (optional).
    d. Select an **Attack Stage** from the dropdown (optional).
6. Use the sliders to set the **Severity** required to trigger the alert or adjust the **Confidence.**
7. In the **Options** section, select the **Only trigger if search matches** box if you want to specify the number of search matches required to trigger the alert.

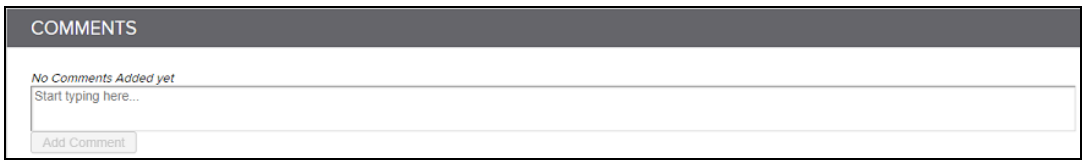
8. Select an operator and enter the number of times required to trigger the alert. For example, if you select greater than **>** and enter 10 times, you will get one alert for every 10 times the search results are matched.



Using Comments

Use **Comments** to view and add comments. You can see all comments and the name of the user who entered them.

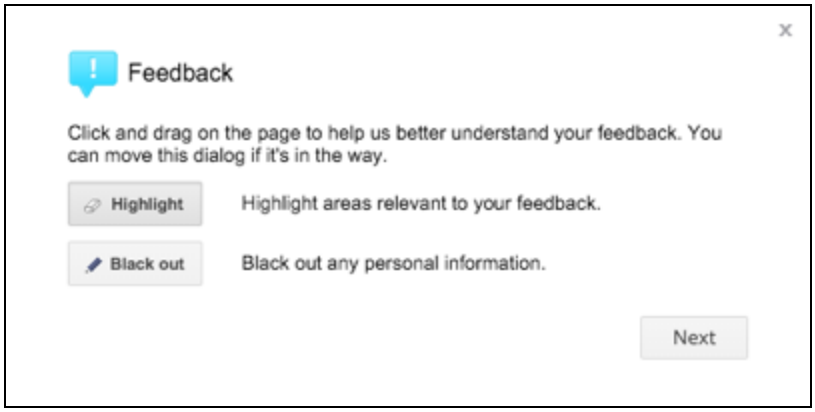
To add a comment, enter text in the box and click **Add Comment**.



Sending Feedback

Click **Send feedback** to send information to Aruba about issues you encounter. This button is available on the bottom right of every screen.

In the first screen, select the areas of the view that you want to send to Aruba.



To highlight an area:

1. Click **Highlight** to activate the highlight tool.
2. Click and drag to select the area of the screen you want to highlight.
3. Click **Next** to move to the next screen.

To black out an area:

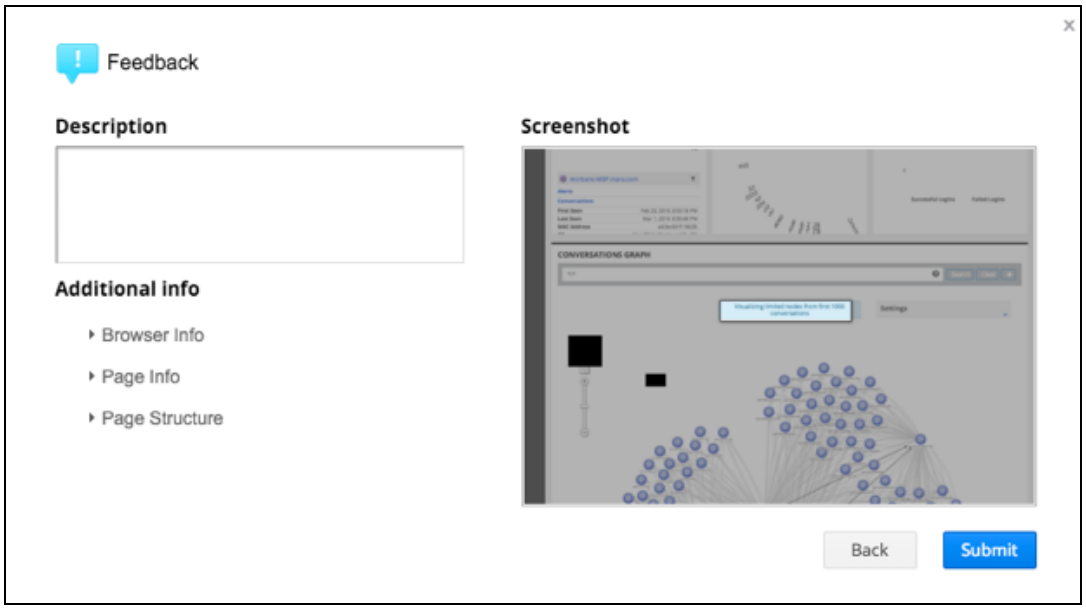
1. Click **Black out** to activate the blackout tool.
2. Click and drag to select the area of the screen you want to black out.
3. Click **Next** to move to the next screen.

NOTE

You cannot apply highlight and blackout to the same area. Both are optional, and you can move between them until you are ready to click Next and move on.

To submit your feedback:

1. Enter a description (optional).
2. Click **Submit**. Be sure to include the information listed under **Additional info**.



Using the Overview

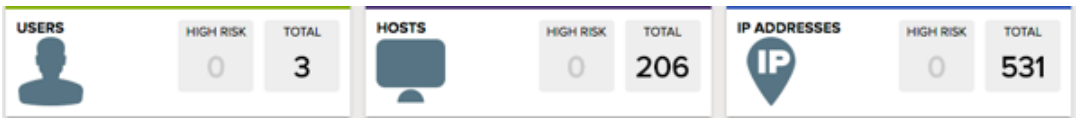
Use Overview to view and investigate entities by risk score. This screen displays when you first log in, and you can click on the IntroSpect logo from any page to access it. The Overview page displays multiple panes with relevant overview information, and you can interact with elements on the page to filter what is displayed and drill down for more information.

Note: Your administrator may change what page is displayed by default.

Entities At A Glance

The top bar displays the entities and objects used by IntroSpect. You can see total count for each entity, or click on one of the High Risk... buttons to display that entity. The Top [Entities] panel will show the high-risk items for that entity. See View Top High Risk Entities for more information.

Note that destination IP addresses are not entities in the system. Also, there will be a delay before objects are displayed as entities, until after IntroSpect assesses them.



View Top High Risk Entities

Use the Top [Entities] pane to see a view of your entities by risk score and to drill down into an entity.

Use this pane to do these tasks:

- View top high-risk users, hosts, IP addresses, or all entities by their risk score.
- Drill down into an entity for more information.

To change the data view

- Select an option from the dropdown

To view details for an entity

- Click on a link to open the Entity360 page with details.

Top Entities

For top entities and Watchlists, the count of high-risk entities and total for the period are displayed in the header.

Column	Description
Entity	Icon for the object type and name of the object. Click to open Entity360.
Department	User department (displays for user entity only).
Risk Score	The risk score for the entity, based on severity + confidence.
Change	Change in risk score over the selected time period.

View Watchlists

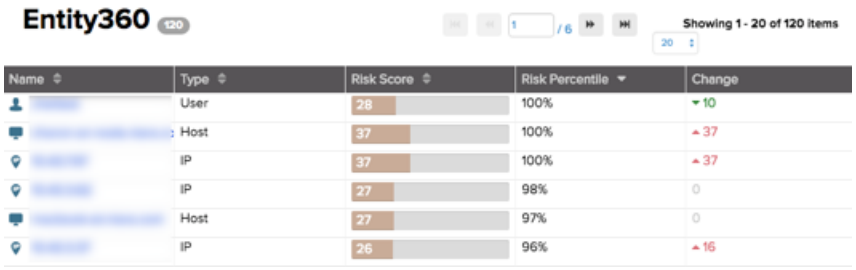
Use watchlists to view custom groups of entities that are shared with you. You can access this feature from the and Entity360 pages. If one or more watchlists exist, you can display them on the **Home** page.

See Configuration—Watchlists for more details.

Use the **Entity360** tab to view a list of entities or drill down into details about entities.

You can view all entities for the time range, or select a watchlist from the dropdown. The number of entities in the search results is displayed next to the **Watchlist** dropdown.

You can also create or manage watchlists from this page.



- To view details for an entity or IP, click the link for the name of the object you want to view.
- To view conversations for an entity or IP, click the **Conversations** link for the object you want to view.
- To view logs for an entity or IP, click the **Logs** link for the object you want to view.

Table 6: *Entity360 Page*

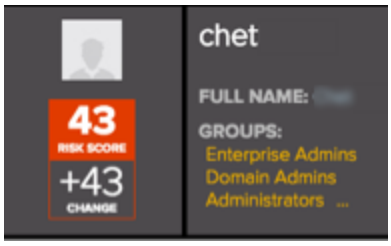
Column	Description
Name	Icon for the object type and name of the object. Click to open Entity360.
Type	The type of object.
Risk Score	The risk score, based on severity + confidence.
Risk Percentile	Percentile ranking of a risk.
Change	Change in risk score over the selected time period.

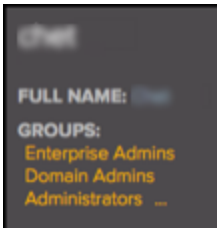
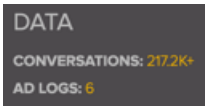
Entity 360 Quick Glance

Once you click on a entity link, from the **Entity360** page or using drilldown to an entity/IP from another page, you see an overview page with information about the entity/IP, and clickable links to drill down for more information.

The bar at the top displays some basic information at a glance, as well as links to drill down for more information. The information will be different for different kinds of entities. It is displayed for all cards.

If you are using Active Directory logs, group information is displayed for users:



Column	Description
	The icon displays the object type (user, host, or IP). The risk score is displayed as red, and the change in risk score over the selected time period is white.
	The Entity name. If a user, additional details display. This is what displays for a user if you are not using Active Directory.
	The user details and Active Directory associations. This is what displays for a user if you are using Active Directory.
	The activities engaged in by the entity or IP. Click on a count to drill down to those items.
	The conversations and logs associated with the object. Click on a count to drill down to those items.

Navigate Entity360 Data

This chapter describes the information and actions available from the main **Entity360** page in the Analyzer UI. The **Entity360** page provides the complete list of all entities in the system as filtered by the available criteria. You can access this page by clicking the **Entity360** icon or from **Menu > Entity360**.

The following options are available from the **Entity360** page.

Time Range Picker: At the very top there is a time range picker. You can set it to a custom time range or any of the other defaults to restrict the scope of the data you are viewing.

Search Bar: There is also a search bar that allows you to type in a search query composed using the IntroSpect search syntax to restrict the set of entities that show up in this list to match any particular search criteria that you might have.

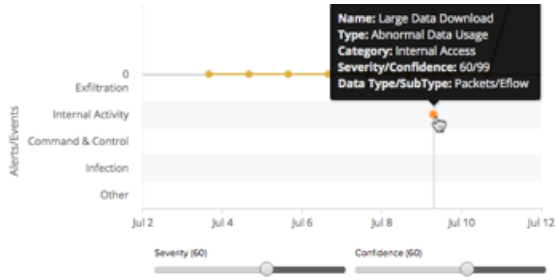
Filter Options: The left navigation pane has various options that allow you to filter and further refine the displayed results. The options include: Type, Risk Score Bucket, Department, and Organization.

Viewing Risk Profile

Use **Risk Profile** to view details for an entity.

- To see risk score for a date, hover over a point on the **Risk Profile** line.

- To see alert details, hover over an **Alert** or **Event**. Click to open the **Alerts** page with details of the alert.



- To see events contributing to a risk score, click on a point on the **Risk Score** line. Data contributing to the risk for for that date displays in a popup.

NOTE

The events contributing to the risk score for that date may not occur on that date, and may also be outside the selected time range.

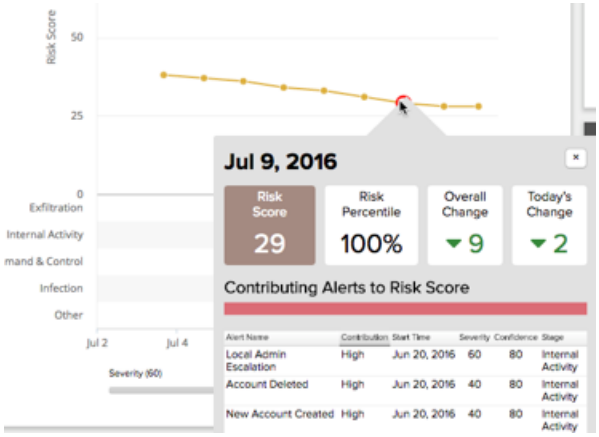


Table 7: *Contributing Alerts*

Column	Description
Type	Type of alert.
Contribution	Level of contribution of the alert to the risk score.
Date	Date or date and time of the event.
Severity	IntroSpect's assessment of the severity of the risk.
Confidence	IntroSpect's confidence in the risk analysis.
Stage	Attack stage. See Alerts By Attack Stage for more information.

Events in Time Range

Events and event summaries for the entity in the time period are displayed next to the **Risk Profile** graph.

Alerts in Time Range

Any alerts for the entity and time period are displayed in another pane next to Risk Profile.

Table 8: *Entity360 Card Summary View*

Left Panel	Button	Description
	actions	Click to export to PDF or assign results to watchlists.
	summary	Click to view entity overview and panes (selected).
	NAC Timeline	Click to view NAC timeline.
	activity	Click to view entity activity summary and trends.
	group by	Click to access groupiong options.
	devices	Click to view device history.
	apps & ports	Click to view applications and ports.
	auth. history	Click to view authentication history.
	conv. graph	Click to view a conversations graph.
	web history	Click to view Web history.
	comments	Click to view comments.

Profile Overviews

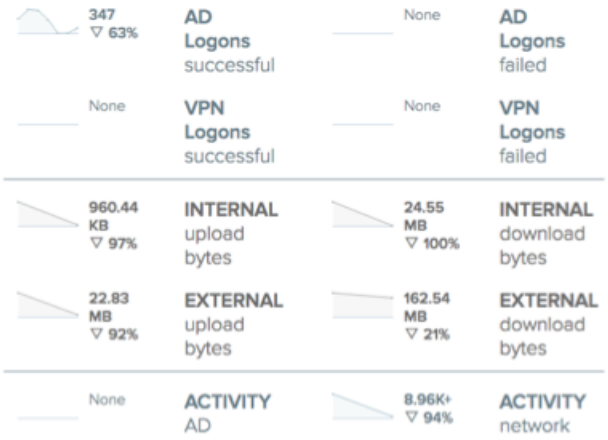
Additional details display for a selected entity, to provide high-level information on usage.

Summary List

The **Summary List** displays a list of the top and bottom usage information for the entity in the selected period.

Trends & Statistics

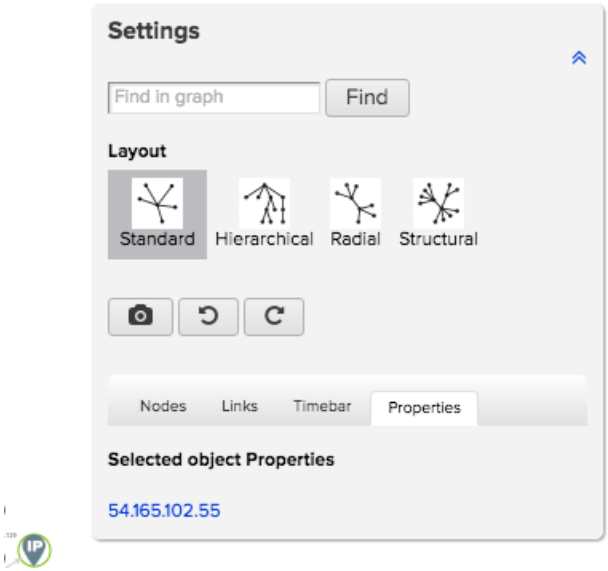
The **Trends & Statistics** pane displays an overview of the activity for the entity in the selected period.



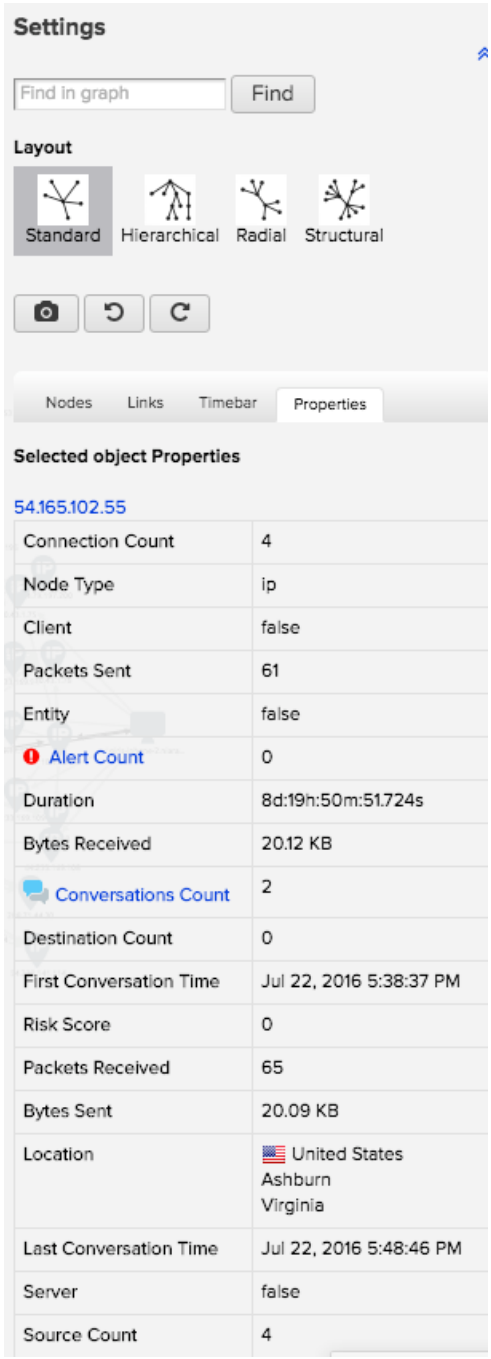
Viewing Device History

Use **Device History** to view all the devices and connections an entity has made, and the hosts and IP addresses contacted by each device.

To view details for an object, click on an object to display it as a link.

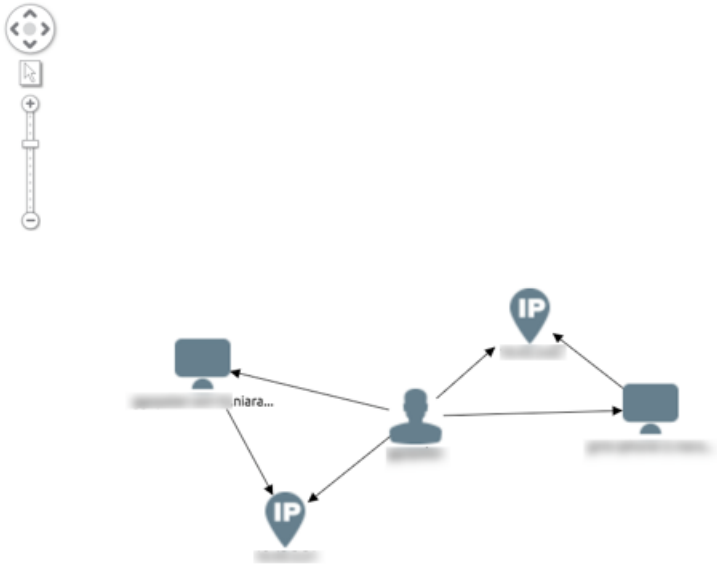


Double-click an object, or click the link in Settings, to display additional details and links to alerts and conversations for the object.



To see a Conversations graph for the filter

Click the filter icon near the bottom right.

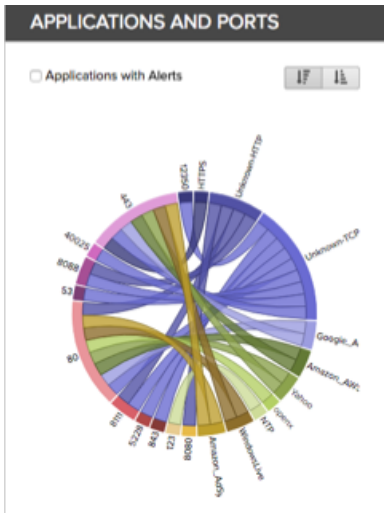


Viewing Applications and Ports

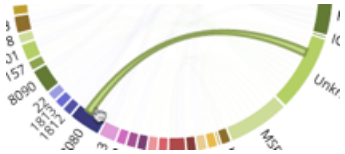
Use **Applications and Ports** to see an overview of protocols used, and to view and drill down into specific connections. You can do this from the small panel on the **All Charts** page, or go to the full **Applications and Ports** page.

You can do the following tasks on this screen:

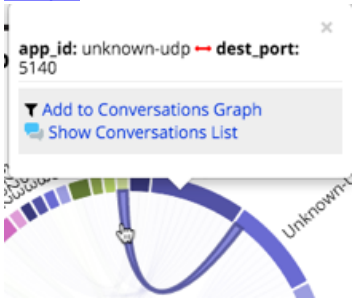
- View applications with alerts.
- View a specific connection and investigate.
- Display either top or bottom group of applications using the controls .



- To view applications with alerts, select the **Applications with Alerts** box.
- To view details for a connection, hover over a line, port, or application.



- To access additional options, click on a connection. You can add the conversation to the Conversations Graph, or see the list of conversations for the connection.

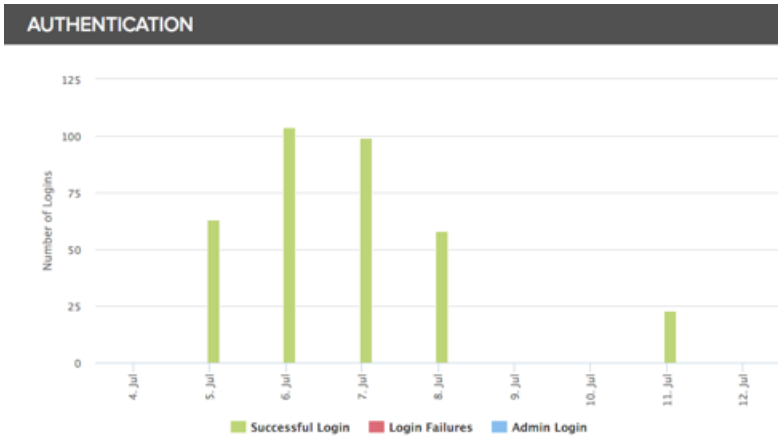


- To add an item to the graph, select **Add to Conversations Graph**.
- To go to the list of conversations, select **Show Conversations List**.

Viewing Authentication History

Use **Authentication History** to view login information at a glance and for specific dates.

Dates are displayed along the **x axis**, and login count on the **y axis**. Each bar displays number of logins on that date – green if successful and red if failed. Blue indicates an Admin login.



Click the icon to open the full page and see additional details in a table below the graph.

Table 9: *Login Details*

Column	Description
Time	The time and date of the login attempt.
Domain	The domain where the login originated.
Host Name	The name of the host where the login originated.
IP Address	The IP Address where the login originated.
MAC Address	The MAC Address where the login originated.
Logon Type	The type of login.
Status	The login status (**Success** or **Failure**).

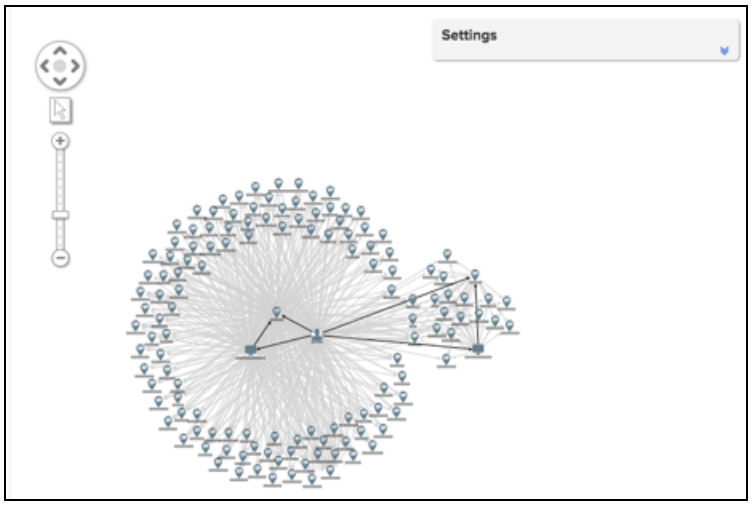
Viewing Conversations Graph

Use **Conversations Graph** to view an overview of the conversations for an entity.

NOTE

The graph shows only the 1000 most recent conversations, which covers only a small amount of time. For best performance, use search criteria to refine the results. You may also want to keep the date range set to past hour or today, unless you use extensive search criteria.

You can refine what is displayed in **Conversations Graph** and the **Timebar** using Options.



Conversations Graph Options

Use **Options** to change what is displayed and how the graph appears.

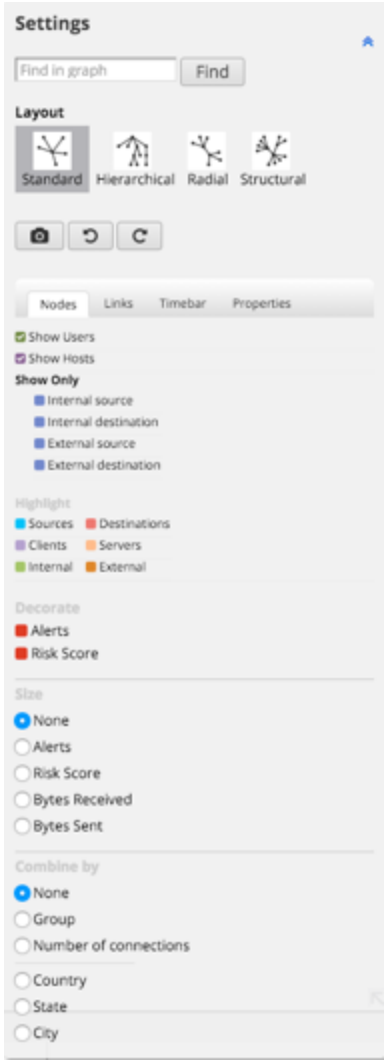
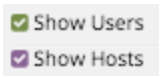
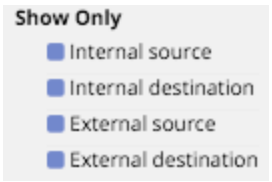
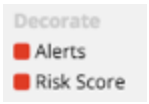
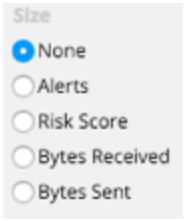
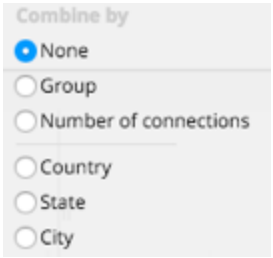


Table 10: *General Settings*

Section	Description
	Enter a host, user, or IP and click Find.
	Click on a layout to change to that view.
	■ Click the camera to capture a displayed state. It will appear in the Captured States list. ■ Click undo to reverse the most recent action. ■ Click redo to reverse the most recent undo.

Table 11: *Nodes Tab*

Section	Description
	Check the box(es) for the entities you want to display in the graph.
	Check the box(es) for the source(s) and destination(s) you want to see in the chart.
	Check the box(es) for the items you want to see highlighted in the chart.
	Check the box(es) to display counts for that object.
	Click an option to resize the circles on the graph according to the selected size criteria.
	Select an option to combine by. The nodes will be displayed by this criteria, with a number displaying the count for the node criteria. Note that internal nodes and connections will not display countries, states, or cities.

Links Tab

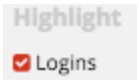
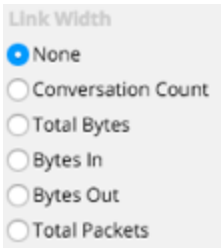
Section	Description
	Check to show link labels, clear to hide.
	Check to display logins. Red arrows will show where logins occurred.
	Select the option you want to display. The width of the connection line corresponds to the size of the metric you set here.
	Select or deselect the types of links you want to see. Click Combine links to group the display of the same link types to different ports. Note, to use these together click Combine links, and then select or deselect the link types, since once you combine all link types are selected again.

Table 12: *Timebar Tab*

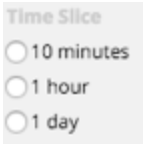
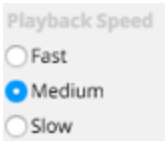
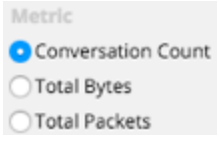
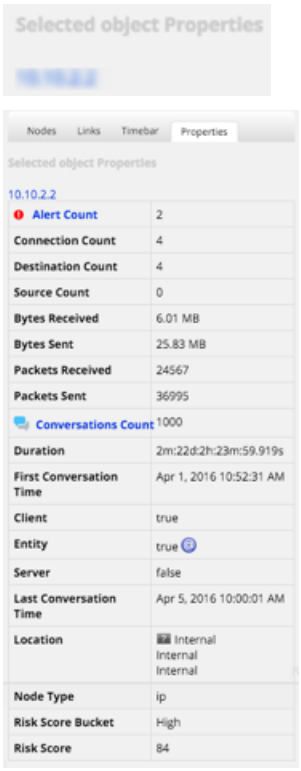
Section	Description
	Select the time slice you want to appear in the Timebar.
	Select the playback speed for the Timebar.
	Select the metric used by the Timebar.

Table 13: *Properties Tab*

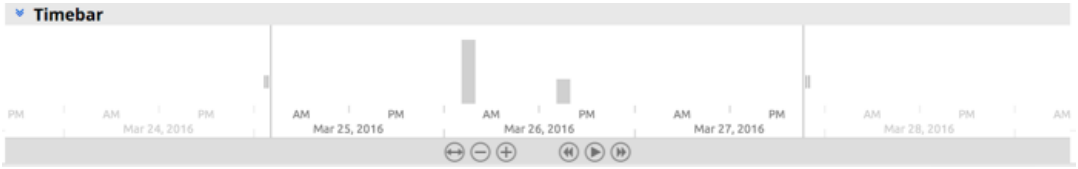
Section	Description
	Click on an object in the graph to see a link to its details. Click the link to open the details window.

Using The Timebar

You can modify the Timebar directly or using the Options. The main graph will update as you make changes. Play the timeline to see the conversation movement in the graph. Scroll or drag the Timebar to see different information.

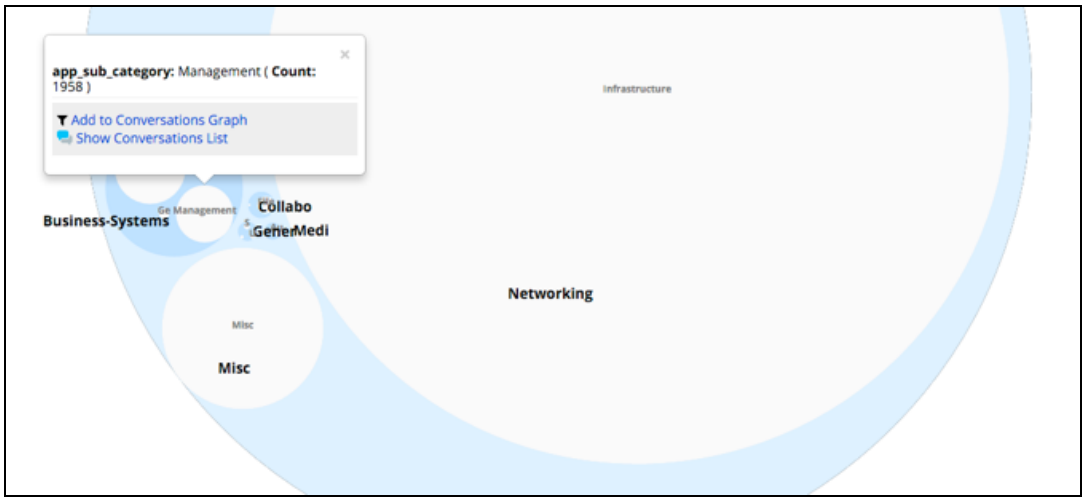
- To view conversation counts, hover on a gray bar to see the count for that time.

- To change time parameters, drag a handle to change the start or end time of the conversations displayed in the graph.
- To reset conversation timeline, click to reset the conversation start to the time period start.
- To zoom, click the + or - buttons.
- To run the timeline, click to play the timeline on the graph.
- To move back or forward on the timeline, click or .



Viewing Web History

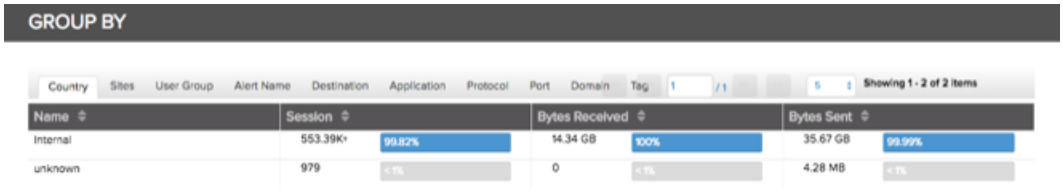
Use Web History to view a web history overview for a selected entity, and to add selected web history types to the Conversations Graph.



- To add an item to the graph, select **Add to Conversations Graph**.
- To go to the list of conversations, select **Show Conversations List**.

Grouping Conversations

You can see individual components of the conversations for your entity, such as country, user, and destination.



To use the **Summary** section, click a tab to see all the conversations in that group.

Use Alerts to view and investigate alerts and related information. You can do the following tasks on this page:

- Filter alerts.
- Drill down into alerts.
- View related entities.
- View related conversations.
- Take actions or make comments on alerts.

Use the search bar to:

- Create, save, and export queries.
- Create Rules.
- Create Notifications.

See Using Search Features for common search features in IntroSpect 2.4 .

Some search features are different in the Alerts page. See Use Alert Search Actions.

Alert Classification

A hierarchy of alert information is displayed about alerts in IntroSpect 2.4 [[[Undefined variable General.Product]]], which will help users understand alert specifics at a glance.

First, alerts are grouped by attack stages, then other groupings cascading down:

1. Attack Stage
2. Alert Category
3. Alert Type
4. Alert Name

Attack Stages

- **Infection**—Activity that would potentially suggest an infected user or host, for example suspicious file downloads.
- **Command & Control**—Abnormal activity indicating communication between a compromised user or host and an infrastructure used to control malware.
- **Internal Activity**—Abnormal internal activity such as privilege escalation, lateral movement, or abnormal resource access.
- **Exfiltration—**Abnormal external activity, such as large uploads to cloud applications.
- **Other—**Activity that is anomalous but not assigned to attack stages. For example, user connecting to websites using expired certificates.

Use Alert Search Actions

Use Alerts search **Actions** menu to search for alerts, and to create rules and notifications.

- There are additional and different search options on the **Alerts** page than those on other pages.
  - To perform the search, click **Enter**.
  - To clear the search and any filters, click in the search bar. Note it is very light until you hover over it.

- Additional options are available from the Actions menu. You can also create Rules and Notifications.

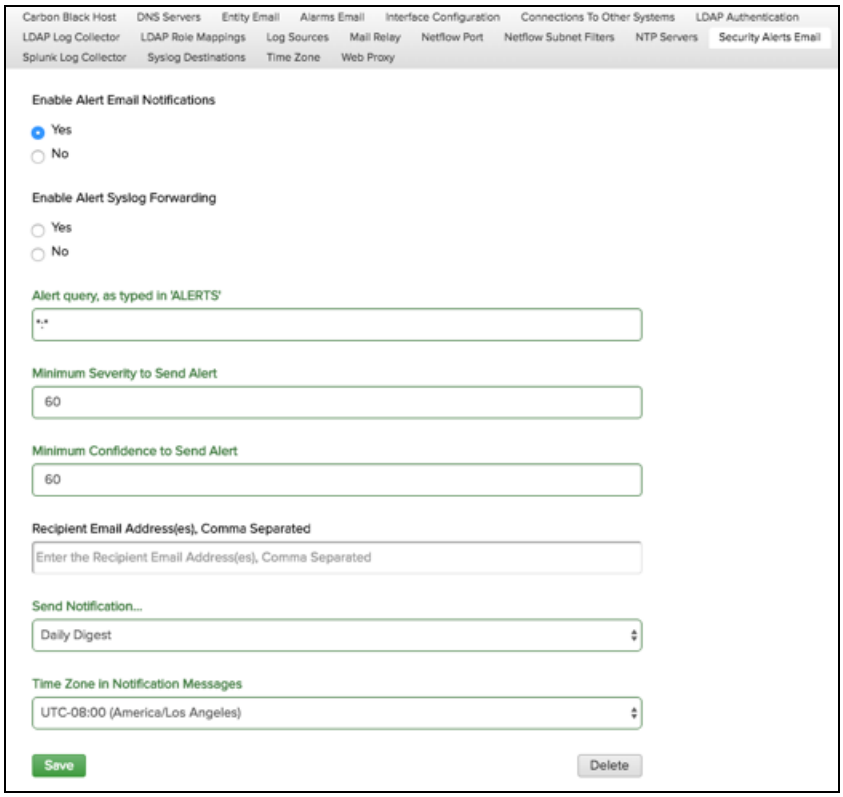
  - To save the search, click **Save query**.
  - To export the search, select **Export to CSV** or **Export to PDF**.

Create Alert Notifications

Use the Alerts search **Actions** menu to create notifications.

To create notifications, select **Create Notification** OR click > **System Configuration > Security Alerts Email** and fill out the form. You can either send email notifications, or send alerts directly to a syslog.

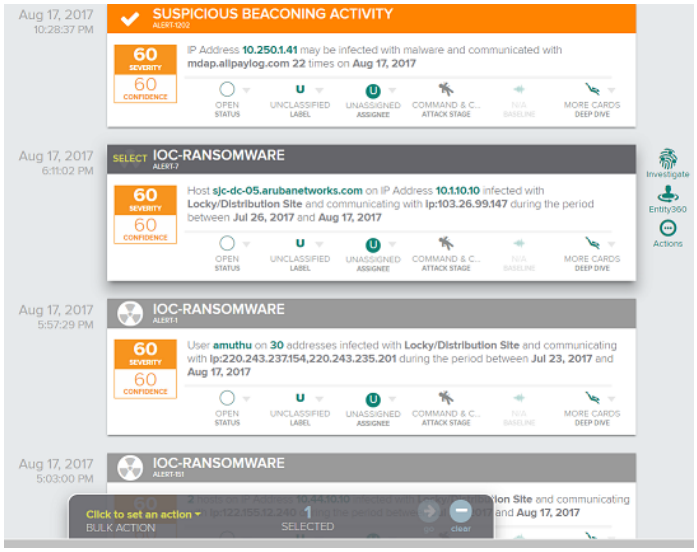
1. Select whether to enable notifications.
2. Select whether to enable Alert Syslog Forwarding (to send alerts to a third-party syslog viewer).
3. Enter or paste the search criteria used to create the alert.
4. Enter the minimum severity required to send an alert, either to syslog or as an email notification.
5. Enter the minimum confidence required to send an alert, either to syslog or as an email notification.
6. Enter one or more recipient email addresses, separated by commas.
7. Select a frequency for sending email notifications.
8. Select the time zone to display in notification emails.
9. Click **Save**.



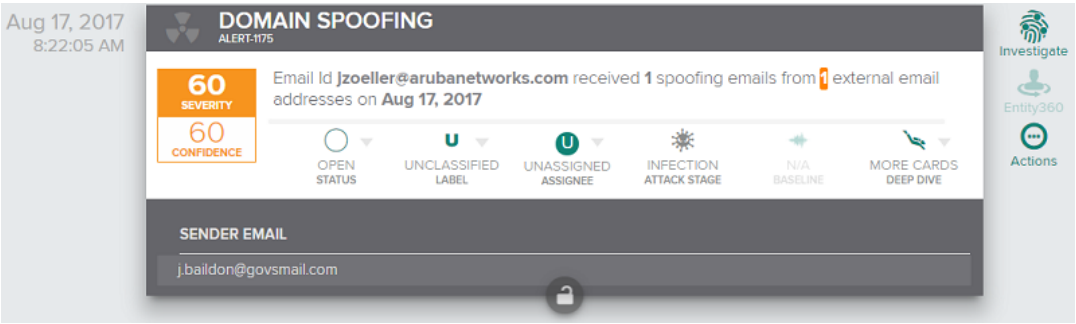
Manage Alerts

The Alerts page displays cards with information about the alerts that meet your search criteria. You can view additional and related information, and take action on the alert.

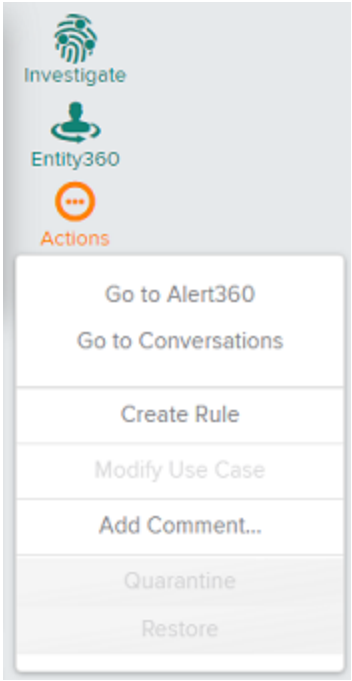
- Click on one or more card headers to select them. Options to apply bulk actions are available at the bottom of the page for the selected alerts.



- Click on a count to display details.



- To view more information about an alert, click Alert360  .
- To view information about the entity involved in an alert, click Entity360  .
- To take action on an alert, choose an option from the **Actions** menu  .
- Click **Add Comment** to add text as a comment.



Using Alert360

Use Alert360 to view, investigate, and take action on an alert.

The panels on this page are explained in this section.

Different panels appear for discrete versus GUEBA alerts and different alert conditions.

Alert Overview

Use the **Alert Overview** panel to:

- View alert information.
- Modify the alert search results.
- View **VirusTotal** information.
- Take actions on an alert.

Modify Search

Click on a field for an alert and use the popup to make changes. The results initially displayed on the main Alerts page will be modified by your selections.

See also Search Using Fields.

To modify the times for the search:

1. Click **Set as Search Start Time** to change the start time for the search to the selection.
2. Click **Set as Search End Time** to change the end time for the search to the selection.
3. Click **New Search as Start Time** to create a new search using the selected time as start time.
4. Click **New Search as End Time** to create a new search using the selected time as end time.

To view information from **VirusTotal**, click the icon in Destination to open the VirusTotal page for the destination.

The Alert columns represent logical hierarchical groupings, as outlined in Alert Classification.

Table 14: *Alert Overview*

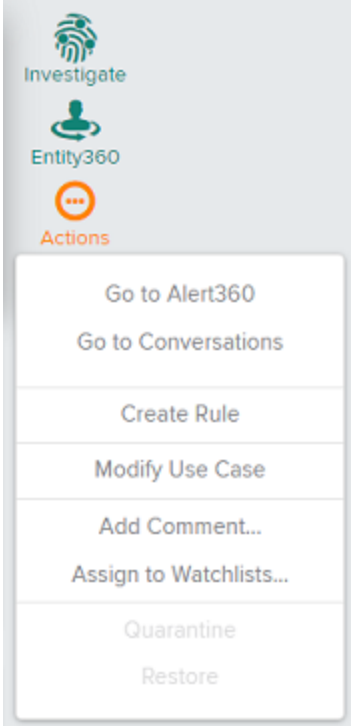
Column	Description
Alert Type	Logical group of alerts within an alert category.
Alert Name	The specific alert in the alert type group.
Alert Category	Broad classification of the threat vector used within an attack stage, based on a combination of data source and method.
Source	The origin of the event that triggered the alert (alert event).
Destination	The target destination of the event that triggered the alert.
Start Time	The time the alert event started.
End Time	The time the alert event ended.
Detected	The date the alert event was detected.
Status	Whether the alert is open or closed.
Assignee	User to whom the alert is assigned.
Actions	Menu of actions to take on the alert.

Take Actions on Alerts

Use the **Actions** menu to take action on an alert.

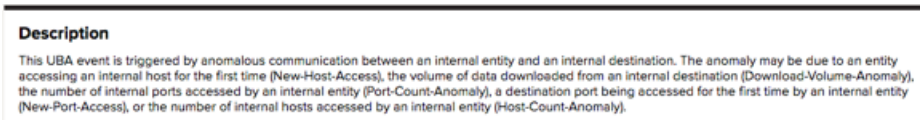
To take action on an alert, choose an option from the **Actions** menu.

- Click **Add Comment** to add text as a comment.



View Alert Description

Use the description field, if it appears, to view information about what triggered the alert, and why it is considered a possible threat.



View Entity Alerts Timeline

Use the **Entity Alerts Timeline** section to:

- View alert occurrences in a timeline.
- View information about an event.
- Open **Alerts360** for an event.
- Adjust the **Severity** or **Confidence** sliders to change which alerts are displayed.

Each alert is displayed on the timeline as a dot in the time and attack stage where it occurred. The current alert is displayed in black, and other alerts display in their corresponding severity colors.

- To view information about an alert, hover on a dot.
- To view alert details, click on a dot.
- To change which alerts are displayed, move the **Severity** or **Confidence** sliders.

Indicators of Compromise

For discrete alerts involving an IOC, several more sections display on the Alert360 page.

NOTE

Not all discrete analytics involve an IOC.

- Use **Primary IOC** to investigate the alert, including:
- See the primary Indicator of Compromise type and details for the alert.
- Check the **VirusTotal** information for the IOC.
- View other users that went to the domain or interacted with the IOC. See IOC Users

IOC alerts are for discrete events such as suspicious PDFs or Portable Executables (PEs). The system finds a filename or file hash that is a suspect IOC. Use the **VirusTotal** link to check whether it is actually a suspect site that's been reported.

Table 15: *Primary IOC*

Column	Description
IOC Type	The type of object identified as the primary indicator of compromise.
IOC	The actual object or event identified as the primary indicator of compromise, such as URL or IP.
	Click to view **VirusTotal** information for the IOC.

See IOC Users

Use this section to find other users that interacted with an IOC. This allows analysts to dig down into details and find other potential risks or users.

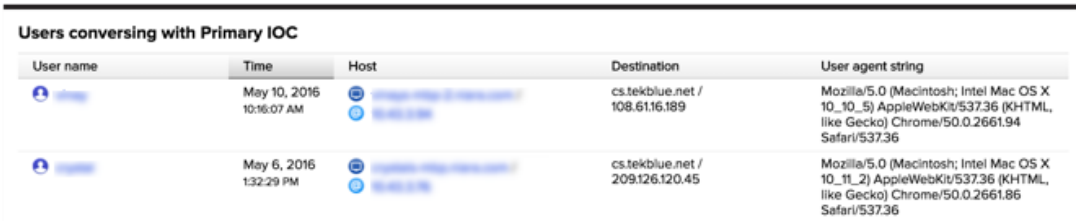


Table 16: *Users Conversing with Primary IOC*

Column	Description
User Name	The name of the user that interacted with the IOC.
Time	The time of the interaction.
Host	The URL and IP address where the communication was hosted.
Destination	The target URL and IP address where the communication was sent.
User agent string	Text string with detailed information. See http://www.useragentstring.com.

Set Alert Related Queries

Use this section to filter by any criteria available for the alert. The options that appear by default are based on the data that contributed to the alert.

- Select or deselect options to include or exclude them from the results displayed, and from the PCAP download. The selected criteria displays in the panels below this section, and updates immediately when you make a change. If you change the time span, the selections revert to the original defaults that contributed to the alert.
- Click on a link to see details for that component.
- Click Get PCAP to download the PCAP for your query results. The file will be available from the Downloads page once completed.

Use Conversations Timeline

Use **Conversations Timeline** to view details of conversations related to the IOC. You can view the cause of the alert, the frequency of conversations, and drill down to see other users who may be affected.

The system does periodic checks, so you can quickly see frequency and number of conversations involved in the alert. Many dots on the timeline following an IOC alert may indicate unusual activity on the network, for instance.

Information and links for conversations are shown in the table.

See Viewing Conversations Graph for information on the graph displayed on this page.

To view details for a conversation, hover over a dot in the chart.

Conversations Table

Use the table to view the conversations and details in a list, and to drill down into a particular conversation.

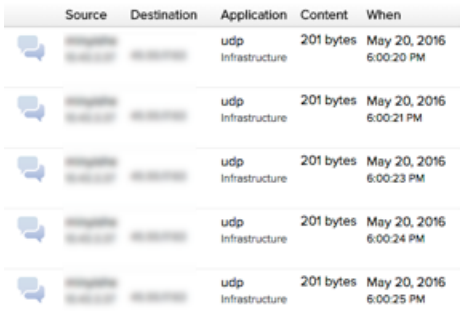


Table 17: *Conversations Table*

Column	Description
	Click to open the Conversation Details page for the conversation.
Source	The originating point for the conversation.
Destination	The conversation's destination.
Application	The application used in the conversation.
Content	The size of the content transferred.
When	The date and time the conversation occurred.

View Alert Audit Trail

Use the Audit Trail section to view the history of actions and changes on the alert.

Table 18: *Audit Trail*

Column	Description
Action	What was changed for the alert.
Update Time	The date and time that the change was made.
Modified Field	Which field was changed.
New Value	The new value for the changed field.
Modified By	The user who made the change.

Use **Conversations** to view information about and drill down into conversations on your network.

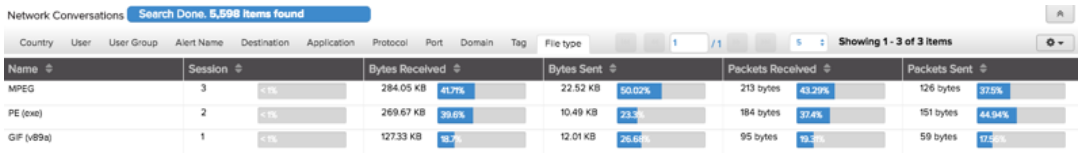
See Using Common Features for common features in IntroSpect.

You can see individual components of the conversations in your filter, such as country, user, and destination.

Use ⌄⌄ or ⌃⌃ to show or hide the **Summary** groups. You may need to expand your browser to see this option.

To use the **Summary** section:

1. Click ⌄⌄ to show or ⌃⌃ to hide the summary groups.
2. Click a tab to see all the conversations in that group.



3. Use the list to filter and view conversations, select one ore more conversations for action, and to drill down into Conversation Details for a conversation.

4. Click on a field in the table to see additional information for the field or apply actions.

Table 19: *Conversations List*

Column	Description
☑	Select for one or more rows to apply options from the Actions menu.
Time	Date and time the conversation occurred. Click the icon or the date to open Conversation Details.
Source	The IP and port where the conversation originated.
Data Source	Type of data used in the conversation.
User Groups	Active Directory user groups involved in the conversation, if this information is available.
Dest Location	The geographic area where the conversation was sent.
Destination	The specific domain name, IP, and port where the conversation was sent.

Column	Description
Application	The application or protocol used in the conversation.
Content	The amount of data downloaded (indicated by a down arrow) and uploaded (indicated by an up arrow).
Summary	What happened in the conversation (that the system knows about), including: ■ Count (number) of transactions in the conversation, if there were multiples. ■ Method used by the conversation. ■ Content type transferred in the conversation. ■ Any failed transfers. Use the information in this column to help determine what to investigate further.

See Conversation Details

Use **Conversation Details** to view very detailed information about the conversations on your network. Access this page from **Conversations**.

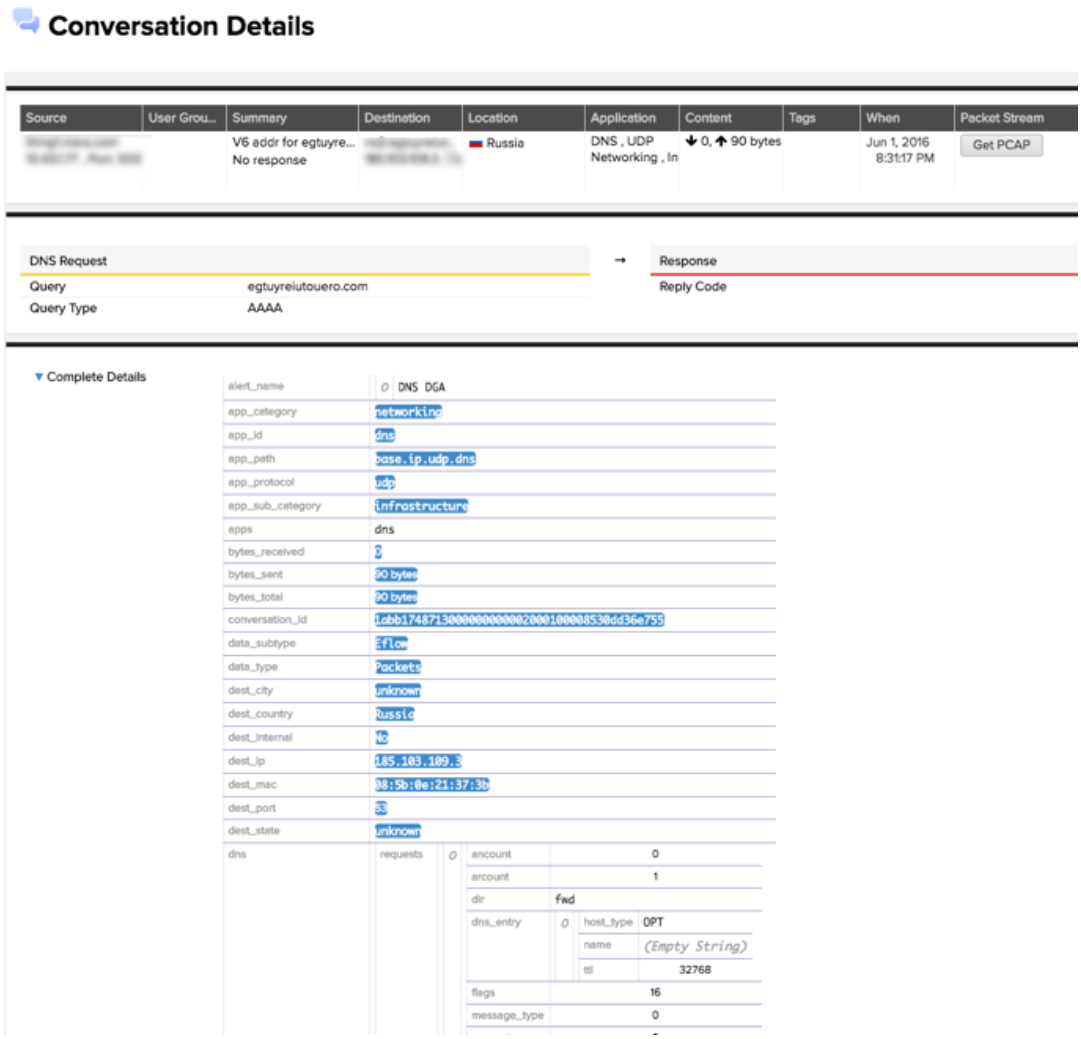


Table 20: *Conversation details*

Column	Description
Source	The IP and port where the conversation originated.
User Groups	Active Directory user groups involved in the conversation, if this information is available.
Summary	What happened in the conversation (that the system knows about), including: ■ Count (number) of transactions in the conversation, if there were multiples. ■ Method used by the conversation. ■ Content type transferred in the conversation. ■ Any failed transfers. Use the information in this column to help determine what to investigate further.
Destination	The specific domain name, IP, and port where the conversation was sent.
Location	The geographic area where the conversation was sent.
Application	The application or protocol used in the conversation.
Content	The amount of data downloaded (indicated by a down arrow) and uploaded (indicated by an up arrow).
Tags	Metadata about the alert for the conversation.
When	Date and time the conversation occurred.
Packet Stream	Click Get PCAP to create a PCAP download with the data exchanged in conversations. The file will be available from the **Downloads** page once completed.

Request and Response—This section displays extensive details about the network interactions, displayed by request and response.

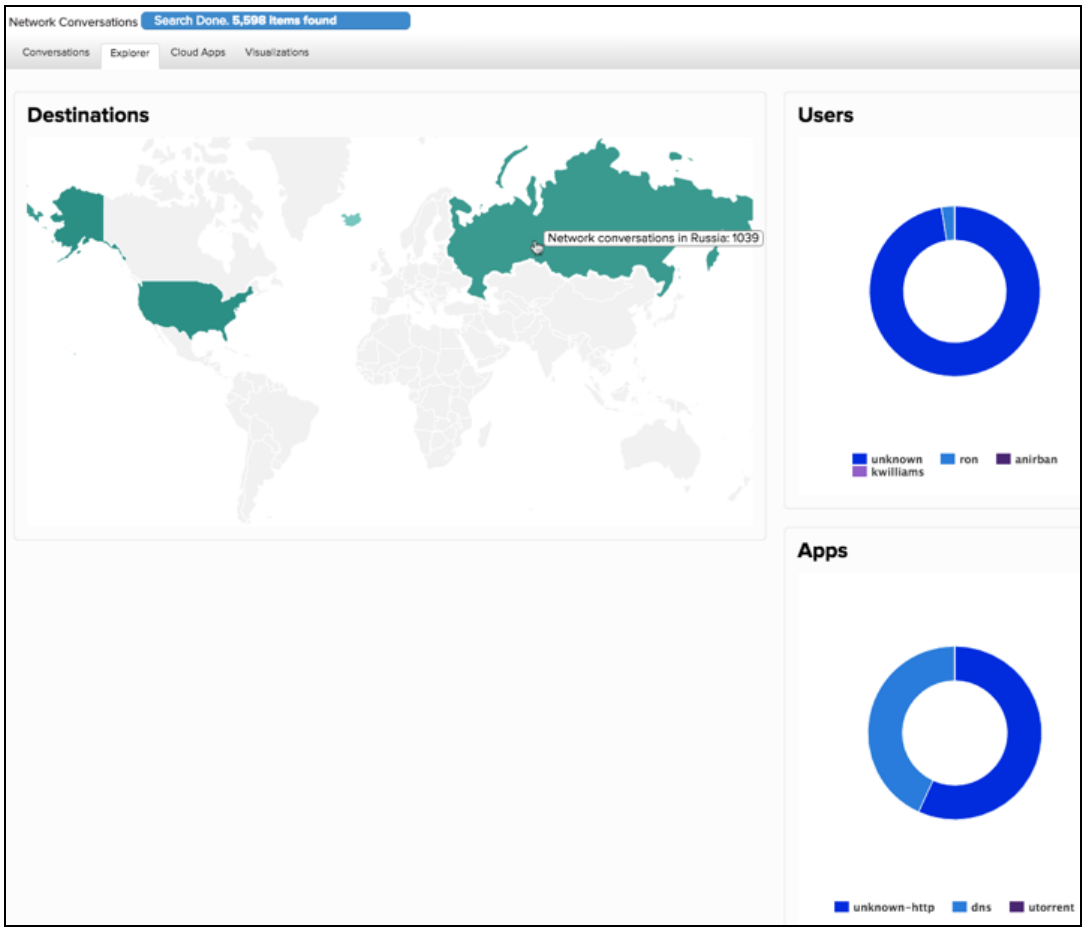
Extracted Objects—This section displays objects that we have and that are relevant. Click to see the object, if available.

Complete Details—This section displays complete raw details from conversations. This is helpful in hunting and investigation; For example, you may want to get the PCAP for a conversation that you notice has gone to Russia.

Conversations Explorer

Use the Explorer sub-tab to see graphs of destinations, users, and apps.

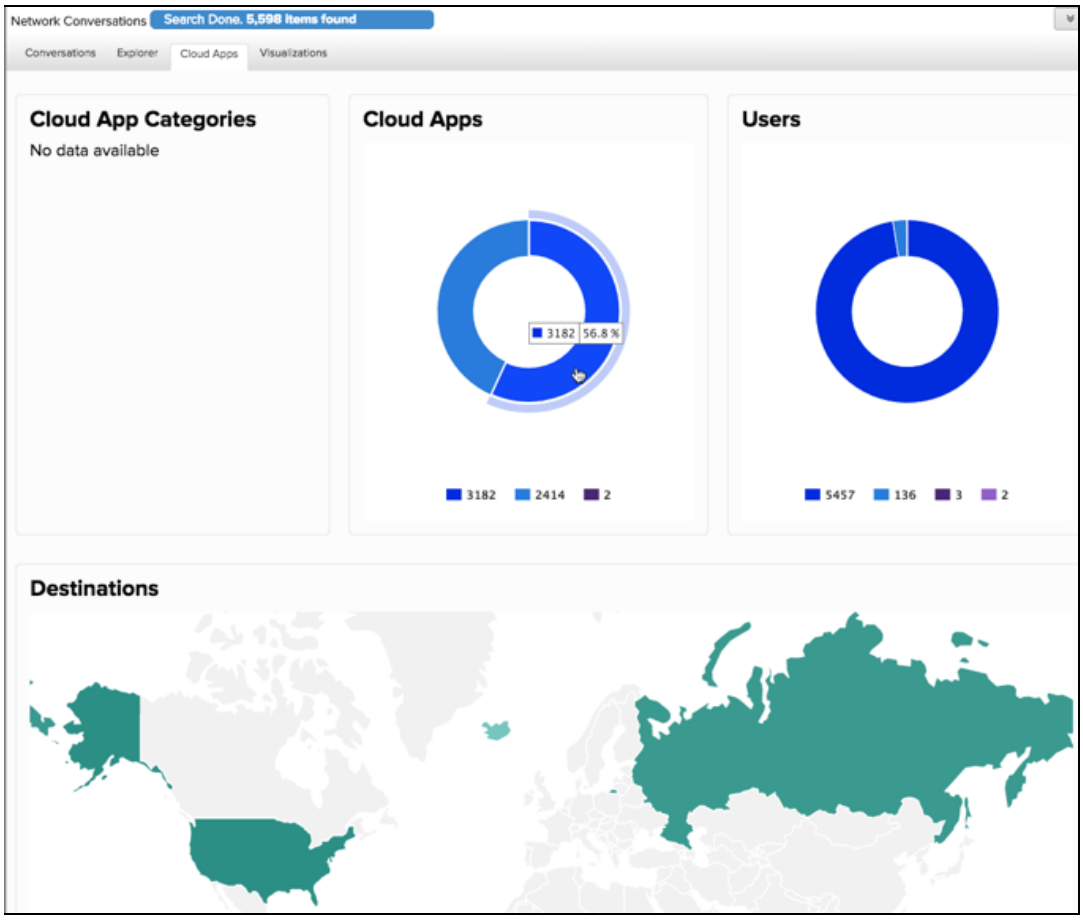
Hover over a colored area to view general information, or click to view only data for that selection.



Conversations Cloud Apps

Use the Cloud Apps sub-tab to see graphs of cloud apps, users, and destinations. (missing or bad snippet)

Hover over a colored area to view general information, or click to view only data for that selection.



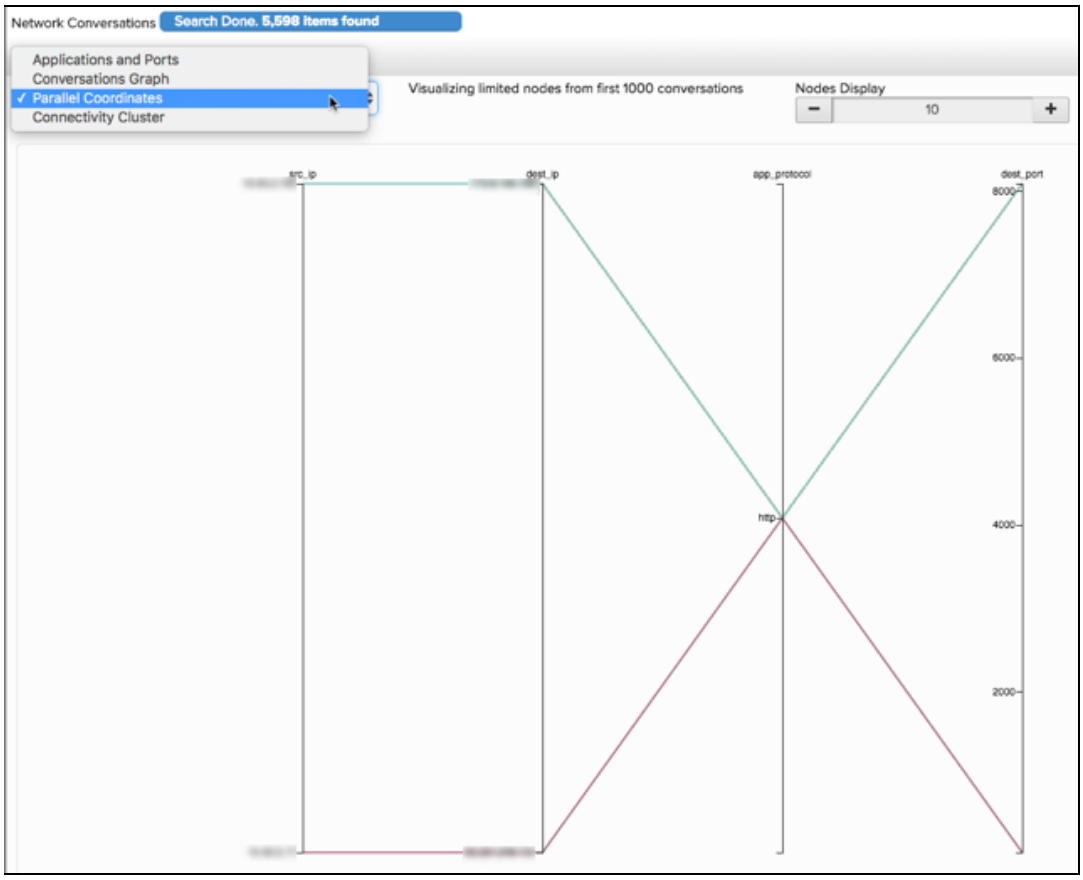
Conversations Visualizations

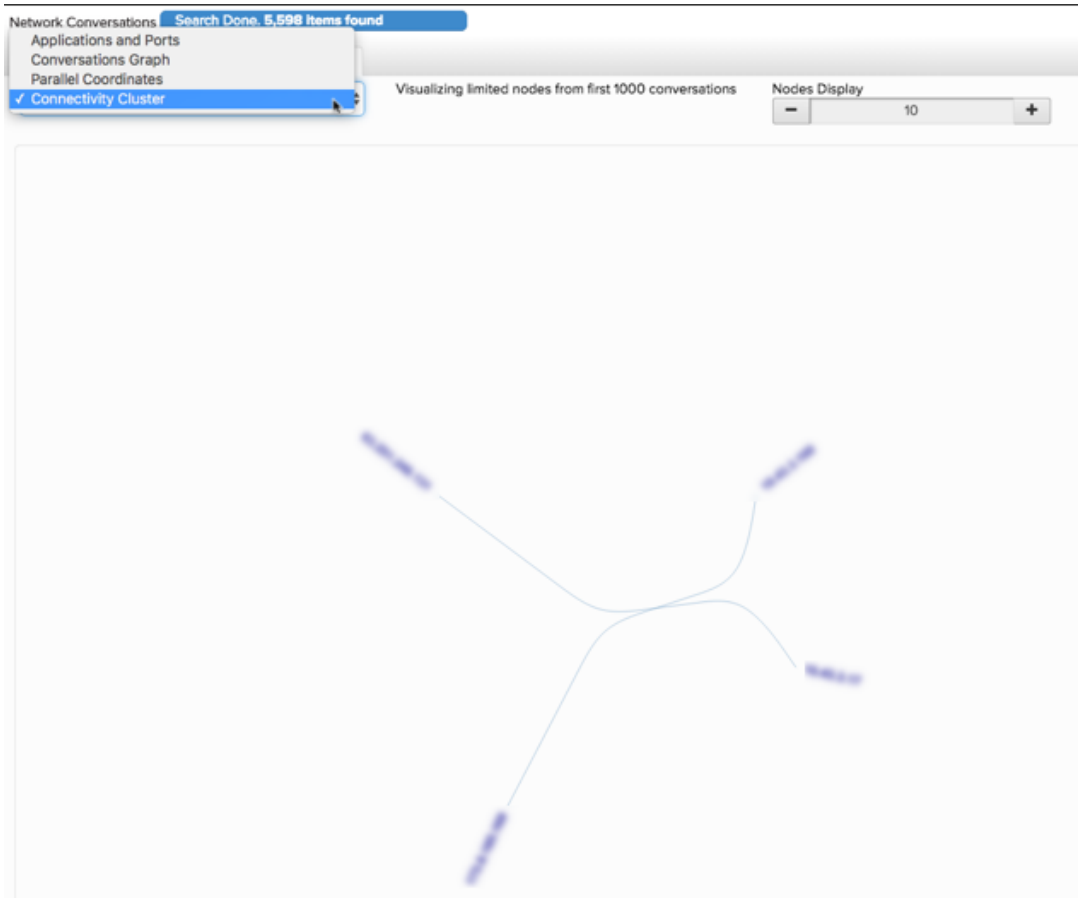
Use the Visualizations sub-tab to see visualizations of network conversations, including:

- Applications and Ports
- Conversations Graph
- Parallel Coordinates shows the contributions of objects on destinations.
- Connectivity Cluster also shows object contributions, but in two dimensions.

To get the most from this information, create a relevant query and then use this section to understand the details.

Select an option from the dropdown for the data you want to view.


Network Conversations
Search Done. 5,598 items found
Applications and Ports
Conversations Graph
✓ Parallel Coordinates
Connectivity Cluster
Visualizing limited nodes from first 1000 conversations
Nodes Display
10
src_ip
dest_ip
app_protocol
dest_port
8000
6000
4000
2000
http

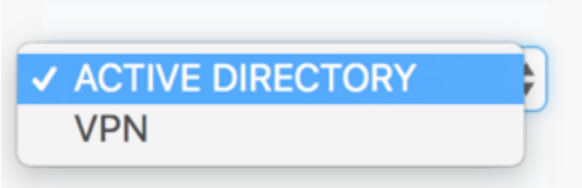

Network Conversations
Search Done. 5,598 items found
Applications and Ports
Conversations Graph
Parallel Coordinates
✓ Connectivity Cluster
Visualizing limited nodes from first 1000 conversations
Nodes Display
10

Use **Logs** to view and investigate your log files. You must first select a log type to view.

NOTE

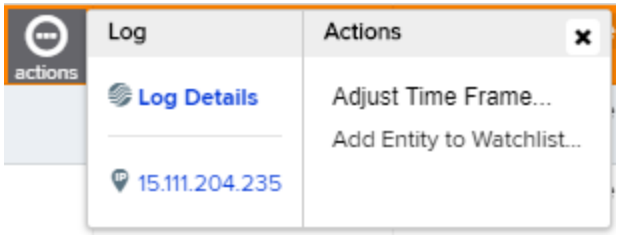
This feature is only available in the advanced version of IntroSpect 2.4 Analyzer.

1. To select a log type, select either **Active Directory** or **VPN** from the dropdown.



2. In the logs page, mouse over the log you wish to view. The highlighted row turns orange.

3. In the **time** column for the row, click on the **log** icon view the log details.
4. For more options, click the **actions** icon.



5. In the **Log** pane, select **Log Details** to view the complete log details.
6. In the **Actions** pane, you can choose to **Adjust Time Frame** or **Add Entity to Watchlist**.

View Log Details

Use the log **Complete Details** to view specific information about a particular log.

To view the complete log details:

1. Mouse over the log you wish to view.
2. In the **time** column, click on the log icon to go to the details page.

Using Search Features

Use the powerful search features in conjunction with Using Filters or on their own. Apply filters to enter them as search queries in the search bar. You can then continue to edit them using additional criteria, and save the search to be used later. You can also use the query language to enter search criteria directly.

Search results counts are displayed while the system is searching. When the search completes, the count is displayed in blue.

Search

Use Search functions to save, clear, or modify your filter selections, or to create new queries manually. You can also view the search documentation.

You can do the following from search:

- View the Search Documentation or searchable fields for a page.
- See your applied filters as a query.
- Manually enter or modify queries.
- Save a search.
- Clear all search criteria, including filters.

Viewing the Search Documentation

To view the search documentation, Click and select an option:

- Click the **Search Documentation** link to open the full document in a new page.
- Click an example link to add the query to your search.

Create or Edit a Query

To create or edit a query:

1. Start entering text for the field you want to use to see the valid entries. You can also enter a space to view all the valid fields.
2. Make a selection from the menu, or enter properly formatted queries manually.

   - To perform the search, click **Search**.
   - To save the search, click **Save** or click the **Actions** menu and select **Save query**.
   - To clear the search and any filters, click **Clear**.

Use **Downloads** to view and manage previous downloaded data and files. You can delete downloads from the list, or download them again. You can also see details and status of downloads.

- To download a file, click the **Download** icon in the **Actions** column for the row you want to download.
- To delete a download, click the **Delete** button in the **Actions** column for the download row you want to delete.
- To delete multiple downloads:
  1. Click in the left column to select one or more specific rows or, to select all rows, click in the header row.
  2. Select **Delete** from the pop-up action bar which appears at the bottom of the screen.

Figure 4 *Downloads*

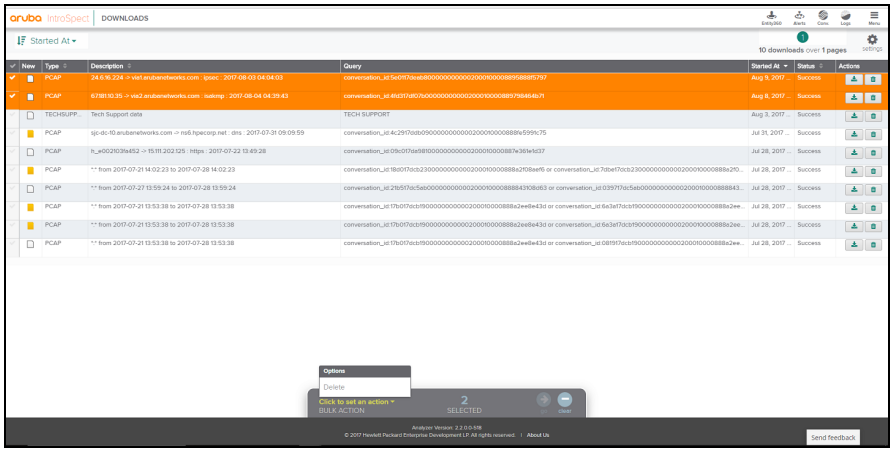


Table 21: *Downloads*

Column	Description
☑	Select rows to download or delete.
New (change to File Info)	Icons indicate: ■ - The query is still running, and the requested download is being created. ■ - The download is available and has not yet been downloaded. ■ - The download has been downloaded previously and is available to download again. ■ - There is an error with the download. Click Refresh from the Actions column to retry.
Type	The file type of the download
Description	
Query	
Started At	Time the download was requested.
Status	Description of the status of the download creation (Success, In progress, or Error)
Actions	Options to download or delete a download

This chapter describes the system information available from the main **System Status** page in the Analyzer UI. The **System Status** page provides a view of the overall health of the system from an operational standpoint. You can access this page from **Menu > System Status**.

The following tabs are available from the left navigation pane of the **System Status** page.

System Status—Alarms

The System Status **Alarms** tab provides a view into all the alarms in the system. An alarm is generated when there is some functional issue with system processes such as ingestion of data, analytics, and others.

The default view is the **Active** view which includes all the alarms that are still active. You can toggle the view to display the **All** view which shows all active and cleared alarms.

If your alarms are configured to generate an email notification when the alarm is raised, you can come to this page and check the status of the alarm: whether it is still active or it has cleared itself. See Alarms Email for more information.

From this tab you can view and assign alarms.

Viewing System Alarms

To view alarms and their detailed information:

1. Go to **Menu > System Status > Alarms**. The default view is the **Active** alarms **List** subtab view which shows all the alarms that are currently active in the system in a grid display.

Figure 5 *List Subtab*

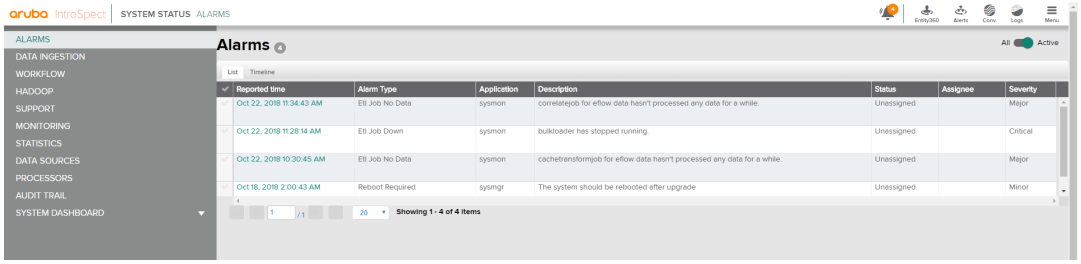


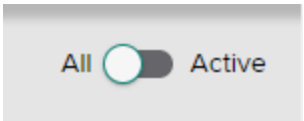
Table 22 lists the details provided for each alarm in the **List** subtab view.

Table 22: *System Status Alarms List View*

Field	Description
Checkmark	Use this column to select a row. You can select multiple rows to perform the same bulk action on all of them, for instance, to clear them all or assign them all to the same person.
Reported time	The time the alarm was reported in the system.
Alarm Type	The type of alarm. For a complete list of alarms, see the *IntroSpect Administration Guide* available on the support site.
Application	The application which generated the alarm.
Description	A brief description of the alarm.
Status	The current state of the alarm.
Assignee	The individual to whom the alarm is assigned for action.
Severity	The severity of the alarm, indicated by the following colors: ■ **Critical**—Red ■ **Major**—Orange ■ **Minor**—Blue

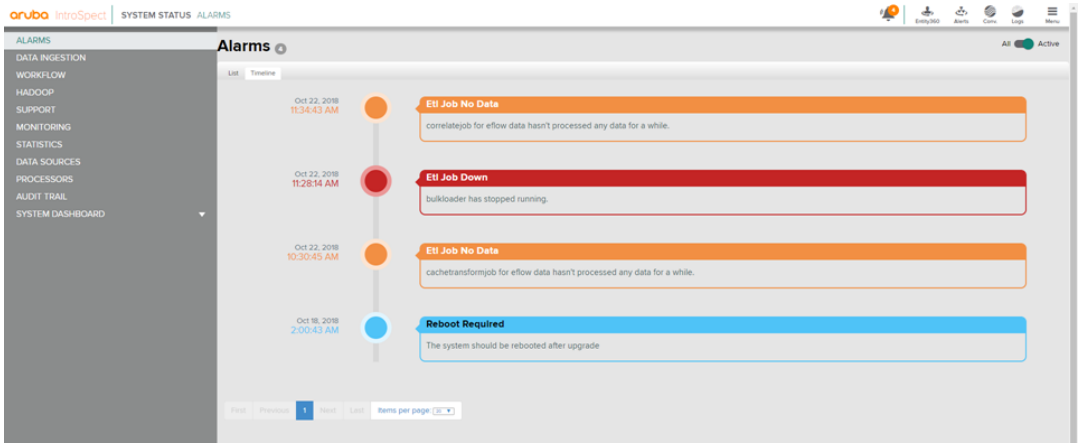
2. To view all the alarms in the system, including cleared alarms, select the **All** toggle.

Figure 6 *All or Active Alarms Toggle*



3. To view the alarms arranged along a timeline, select the **Timeline** subtab.

Figure 7 *Timeline Subtab*



Assigning Alarms from the List Subtab

You can make both individual and bulk assignments of alarms from the **List** subtab view.

To assign alarms:

1. Go to **Menu > System Status > Alarms> List**.
2. The active alarms grid is displayed.

- Click in the checkmark column to select the alarm or alarms that you wish to assign.
- To select all the active alarms in the view, click the checkmark in the column heading.

3. In the **Bulk Action** card that appears, select an option:
   - **Assign to self**—
   - **Assign to...**—
   - **Clear**—
4. Click **Continue** to complete the assignment. You will receive a confirmation message at the top right of the screen.

NOTE

Superuser roles can assign alarms to others for action.

Assigning Alarms from the Timeline Subtab

You can also assign alarms for further action from the **Timeline** subtab view. However you cannot make bulk assignments from this tab:

1. Go to **Menu > System Status > Alarms> Timeline**.
2. The active alarms timeline is displayed.
   - Click the round button on the timeline next to the alarm or alarms that you wish to assign.
3. In the pop-up box, select an option and follow the prompts:
   - **Assign to self**—
   - **Assign to...**—
   - **Clear**—
4. Click **Continue** to complete the assignment. You will receive a confirmation message at the top right of the screen.

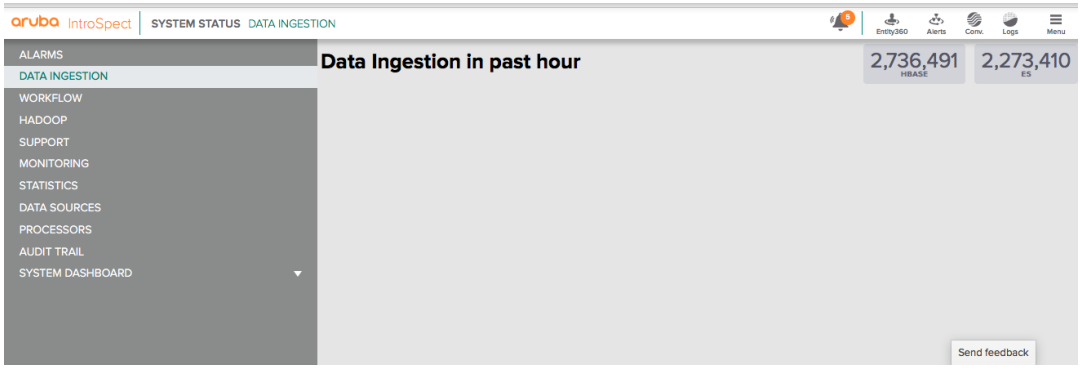
NOTE

You do not need to clear alarms explicitly as most alarms clear themselves when the condition that caused them is no longer in effect. When you clear an alarm, you lose the state of an error condition on the system. It is recommended to only clear alarms that are much older in time when that condition is no longer applicable.

System Status—Data Ingestion

The System Status **Data Ingestion** tab provides view-only information on all the nodes in the Analyzer cluster.

Figure 8 *Data Ingestion Tab*



The two statistics at the top are the counts of the number of records that have been ingested in the past hour into HBase and Elasticsearch. These two counts should essentially be the same. If there is an issue with the

ingestion into these two databases, and these counts are not the same, as in the example figure above, they need to be investigated right away.

Contact Tech Support for assistance with any issues that you may notice here.

System Status—Workflow

The System Status **Workflow** tab provides statistical data about the system's ETL pipeline. This data is presented in visual format through a variety of charts—**Analytics**, **Data ETL**, and **Others**.

This tab is useful for debugging the system, and every time each of these modules touches the data, it records the count of the number of records that have been ingested into the system as well as the amount of time spent by those modules in looking at the data.

This information about the system is useful for the support team in troubleshooting any system issues.

With these charts you can perform the following actions:

- View various system processes against a timeline in increments of thirty minutes.
- Use the **Time Frame** dropdown list at the top of the page to select a period of time for viewing data. You can also use the slider tools below each chart to set a time frame for viewing data.
- Click on a process name to the right of a chart to highlight it on the chart.
- Hover on a node on the graph to view summary information for a batch of data—the batch date, process name, batch run time, and batch ID. You can use the batch ID to locate the batch process information within the logs found in the /var/log/analyzer_sced subdirectory.
- Click on a node to view detailed log information for the batch process in a new page.

Analytics Chart

The **Analytics** chart displays the status of various workflows related to Analytics. It provides data for the following processes:

- GenericUBA
- EventGenerator
- EntityScoring
- EntityAuthProfiler

Data ETL Chart

The **Data ETL** chart displays the status of various workflows related to data processing pipeline. It provides data for the following processes:

- LogIngestionPipeLine
- CacheTransform
- CorrelationBulkLoader
- EflowCorrelation

Others Chart

The **Others** chart displays the status of various workflows that are used for ongoing maintenance of the system. It provides data for the following processes:

- FilePurger
- FeedPipeLine

- ObjectPipeLine
- RuleEnginePipeLine
- RetentionPurgerPipeLine
- CefFeyeCorrPipeLine

System Status—Hadoop

The System Status **Hadoop** tab provides information on some of the modules in the Hadoop platform.

IntroSpect uses several components of the Hadoop ecosystem for storage and data processing. All of the Hadoop operations are coordinated by IntroSpect software. It is not necessary to be aware of the these operations.

Some of the major Hadoop components include:

- HDFS[1]—Hadoop file system for short-term and some long-term storage
- HBase—database for long-term storage
- YARN[2]—Hadoop component to coordinate data processing
- Spark—analytics engine for data processing
- Flume—module used to move incoming log or networking data to HDFS

Flume Summary

Flume Summary statistics provide visibility into the different components (Sources, Channels, and Sinks) that are used by Flume to process data into HDFS. Within Flume, the data flows from Source to Channel to Sink.

The values shown here are meant to be used for debugging purposes and are usually expected to be non-zero values. Depending on the actual data types, zero values can indicate that there is something wrong with the pipeline and some of the data is not being picked up. For instance, AD log information coming from your environment is expected to contain data and not show a zero value.

Sources

A Source is a Flume component which receives data and stores it into one or more Channels.

It is good to monitor these sources and ensure that these stats are incrementing. Events Received, Events Accepted, Batches Received, and Batches Accepted all should be incrementing with time. If one of the sources doesnt increment, it indicates that it is in a bad state and needs to be investigated.

Channels

The next stage in the pipeline within Flume is the Channels.

A Channel is a Flume component which is a passive store that holds the data until it is consumed by a Sink.

The Channels statistics should be non-zero, specifically the Puts Succeeded, Takes Attempted, and Takes Succeeded statistics. The Percentage Full value indicates how full the channel is, and it should never be higher than fifty percent (50%).

Even in heavily loaded systems, these channels should not be very high. High values could indicate that the incoming rate is much higher than Flume can handle, and need to be investigated.

[1]Hadoop Distributed File System

[2]Yet Another Resource Negotiator

Sinks

A Sink is a Flume component which removes data from the Channel and places it into an external repository such as HDFS.

The Sinks should show non-zero statistics for the sink sources that are applicable in your environment. Each of these Channels and Sources are categorized by the type of data. For instance, if you are pulling in Eflow data into your environment, then the Eflow counts should be non-zero. Similarly, if you're pulling in AMON, DNS, or DHCP, or AD user data, their values should be non-zero. Otherwise it indicates some problem in the system.

Flume Activity

In the **Flume Activity** tab, the data is presented in a graphical view over time and shows data being pulled in through the pipeline inside Flume.

The statistics here provide visibility into the different Sources, Channels, and Sinks that are used by Flume to process data into HDFS. These graphs are merely for debugging purposes and should all have periodic up-ticks in data being pulled through the system. Flat graphs have no data and usually indicate that there is something wrong with the pipeline and some of the data is not being picked up. However, it is the actual type of data which helps to determine whether a particular graph should be flat or not. For instance, if you are getting AD log information into your environment, it should be non- zero and you should have graph data for it.

In each category, you can select and deselect these graphs by clicking on the data type names at the top of each graph. To only view a certain type of data, you can deselect all the others and only your selected data is visualized in the graph.

System Status—Support

The System Status **Support** tab is used to extract log data from the system.

To download logs from this tab, select the following options for a log file and then click **Download Logs**:

- **Type**—use this dropdown to select the type of logs. Options include:
  - Web Application Log
  - Data Pipelines Log
  - Installation/UpgradeLog
- **Priority**—use this dropdown to select logs by their priority level. Options include:
  - Critical
  - Major
  - Minor

The type of log as well as the priority of the logs determine which particular log is extracted.

To obtain ETL logs, select Data Pipeline Logs and then Download Logs. The logs are generated and provided in your browser to download to a local file. These Data Pipeline logs can be very large and the download can take a while before you see a dialog to save that file to the local disk.

Installation Upgrade logs and Web Application Logs are smaller.

Tech Support

The **Generate Tech Support File** button generates a very large file containing a variety of different logs and data from the system that can be used by the IntroSpect Support team to diagnose problems.

When the file is available you can go into the download page to obtain all the files generated as part of the Tech Support file.

Analyzer Health Check

The Analyzer Health Check tool runs a system status check on the functionality of the processes that are running as part of the Hadoop ecosystem. It is a useful view into whether everything is functioning as expected in the system. The following status is provided:

- OK or Good—all systems are functioning well
- Bad—some systems are not functioning properly

Example

The typical output on a healthy system looks like the following:

```
Checking if the ambari-agent service is running on the cluster hosts...
... Ok
Checking if the ambari-server service is running on the an-node host...
... Ok
Checking if the ambari-server-db service is running on the an-node host...
... Ok
Checking the management services...
AMBARI_METRICS                 STARTED
...GOOD
... Ok
Checking the cluster services...
FLUME                  STARTED
...GOOD
HBASE                  STARTED
...GOOD
HDFS                   STARTED
...GOOD
MAPREDUCE2             STARTED
...GOOD
SPARK                  STARTED
...GOOD
YARN                   STARTED
...GOOD
ZOOKEEPER              STARTED
...GOOD
... Ok
Checking if the opentsdb service is running on the opentsdb hosts...
... Ok
Checking if the collectd service is running on the cluster hosts...
... Ok
Checking if the analyzer service is running on the an-node host...
... Ok
Checking if the analyzer_sched service is running on the an-node host...
... Ok
Checking if the elasticsearch service is running on the es hosts...
... Ok
Checking if the redis service is running on the an-node host...
... Ok
Checking the Elasticsearch cluster status via host cdh-3...
epoch      timestamp cluster                       status node.total node.data shards pri
relo init unassign pending_tasks max_task_wait_time active_shards_percent
1511771840 08:37:20  cluster-internal-elasticsearch green           3         3    948 474
0    0        0             0                  -                100.0%
... Ok
Checking if the spark-history-server service is running on the yarnrm host...
... Ok
Checking if the hbase-thrift-server service is running on the hbasethrift hosts...
... Ok
```

System Status—Monitoring

The System Status **Monitoring** tab provides statistical views into each of the components that make up the ETL pipeline. It begins from the time data is being pulled from external sources, all the way through to when the data is ingested and populated into databases such as Elasticsearch, HBase, and Parquet. This is useful for determining if there is an issue with the ETL pipeline.

The following charts provide a view of the data for each of the major components of the ETL pipeline.

- Amon
- LogCollector
- Logger
- Log Transform
- Flume
- Cache Transform
- Correlator
- Bulk Loader

System Status—Statistics

The **Statistics** tab of the **System Status** page provides the ability to create custom statistics that can be monitored.

This tab is used by Tech Support to perform troubleshooting and diagnose activity on your system.

System Status—Data Sources

The **Data Sources** tab within the **System Status** page provides a view into the data that is coming in from Packet Processor.

The **Data Sources** tab presents the following information in a grid view:

Table 23: *Data Sources Tab*

Field	Description
Data Name	Data Type name.
Rate	The rate of Eflow data that is generated by the associated Data Type and sent to Analyzer. Depending on the time duration chosen, the average event rate is computed for that duration. Use the time range picker at the top of the page to select a time period and see the computed rate for the selected period.
Health	The smileys indicate the status of the associated Packet Processor: ■ Happy—Packet Processor is connected ■ Sad—Packet Processor is disconnected
Last Time Data Seen	The last time the data was seen from this data source.

System Status—Processors

The **Processors** tab displays information about the Packet Processors in your system and their status.

From the **Processors** tab, you can view and take actions on Packet Processors. For instance, you will need to access this tab when you upload an image file for upgrading the Packet Processor code version from the Analyzer UI (see Configuration—Processor Images).

System Status—Audit Trail

The System Status **Audit Trail** page provides a grid view of all the user activity from the Analyzer UI. It enables administrators to view all users on the system and their activities on a regular basis, with respect to the user records they've been accessing, the queries they've been executing, and the various navigation attempts into the system. Previously executed queries are recorded on the Audit Trail page and you can view and run them again, if needed.

The information presented in the grid view is described in the following table. You can hover over the column headings to access a search field where you can enter a search term to filter the records displayed.

Table 24: *Audit Trail Columns*

Field	Description
Operation	The operation executed in the system.
Status	The status of the operation that was executed.
Username	The username of the account that performed the operation.
IP	The IP address from which the operation was accessed.
When	The time stamp of the operation that was executed.

System Status—System Dashboard

The **System Dashboard** tab provides a view into each of the nodes that make up the Analyzer cluster. There is the main AN, which is the management node, as well as the compute nodes designated by cdh-x where x indicates the number.

- A fixed configuration Analyzer cluster has 3 compute nodes: cdh-1 through cdh-3.
- A scale-out Analyzer cluster has a minimum of 5 compute nodes: cdh-1 through cdh-5.

This tab provides a view into the CPU, network, memory, and all disk utilization on each of these nodes.

Chapter 8
Configuration Page

This chapter describes the various system settings and management options available from the main **Configuration** page in the Analyzer UI. You can access this page from **Menu > Configuration**.

The following tabs are available from the left navigation pane of the **Configuration** page.

Configuration—System

The **System** tab is accessed from **Menu > Configuration > System** and contains numerous subtabs where you can manage specific system configuration settings.

Each subtab and its functions are discussed in the following topics:

Alarms Email

The **Alarms Email** subtab is used to configure system alarms for issues or non-functioning problems on the system. Configure notifications at **Configuration > System > Alarms Email** to receive email notifications about system issues.

The following procedures are described in this section:

Configuring Alarms Email Notifications

Follow these steps to configure systems alarms notification emails.

1. Go to **Menu > Configuration > System > Alarms Email > Add New.**
2. In the **Enable Alarm Email Notifications** field, select an option to enable or disable sending email notifications for alarms.
3. In the **Enable Alarms Syslog Forwarding** field, select an option to enable or disable sending the syslog associated with an alarm. You can configure syslog destinations in the Syslog Destinations subtab.
4. In the **Minimum Severity to Send Email Notification** field, select the minimum severity level at which you want an alarm sent out. The recommended minimum severity level is **Major**.

5. The **Include Hadoop Platform Alarms** option allows you to include Hadoop platform alarms in the notifications. The recommended option is **Yes**.
6. In the **Recipient Email Address(es), Comma Separated** field, enter the email address to which the email is sent. You can enter multiple email addresses, separated by a comma.
7. In the **Send Notification...** field, select the frequency for the alarms email or syslog notifications. You have several options:
   - The recommendation for alarms is the first entry **New Alarms - As produced**. This allows you to be notified right away when there is an alarm condition.
   - The other options accumulate the alarms and send out an email or a syslog in intervals of 10 minutes, an hour, or once a day.
   - You can also specify whether you want an alarm to be sent out when it has been cleared.
8. The **Time Zone in Notification Messages** field, allows you to select the time zone of the timestamp in the notification email. Some considerations include:
   - All data in the backend is maintained normalized to UTC time.
   - If you select your time zone here, the timestamp in the alarm notification emails that are sent out are normalized to your time zone's timestamp.
   - If you have recipients in multiple time zones, it is best to leave it in UTC. However, if you only have email recipients in one time zone, you should specify that particular time zone to make it easier to read.
9. Click **Save** to apply your changes.
10. You can click **Delete** to remove your entry.

Basic Configuration

The recommended basic configuration for alarm email notifications is shown in Table 25.

Table 25: *Recommended Basic Configuration for Alarm Email Notifications*

Setting	Default Value	Note
Include Hadoop Platform Alarms	Yes	The IntroSpect system monitor raises alarms on any major Hadoop malfunction. This check box forwards alarms directly as they are raised by the Hadoop management system, Ambari.
Minimum Severity to Send Email Notification	Critical	-
Send Notification...	New Alarms - As produced	-
Time Zone in Notification Messages	UTC	The timestamps in emails are localized in the specified time zone.

Sending a Test Email

You can click the **Test** button to send out a test email and check the notification that is generated.

Adding Notifications for Cleared Alarms

You can add an email notification for cleared alarms. Alarms clear themselves when the alarm condition is no longer met.

To enable a cleared alarm notification, follow these steps:

1. Go to **Menu > Configuration > System > Alarms Email**.

2. Click the **Add New** button at the bottom of the form.
3. Create an exact copy of the initial notification, except for the **Send Notification...** field.
4. If **New alarms – No more than once every 10 minutes** was used initially, now use **Cleared alarms – No more than once every 10 minutes**.

The **Add New** button can be used to add multiple notifications with different conditions and different destinations.

NOTE

The two notifications—new alarms and cleared alarms—are independent. In some cases, due to notification suppression, it is possible to receive a Cleared Alarm notification even if no New Alarm notification was sent previously.

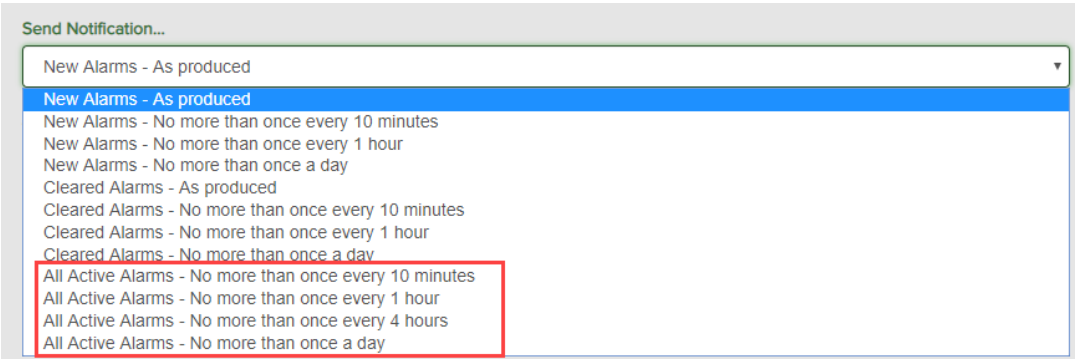
Adding Periodic Alarm Notifications

IntroSpect 2.4.0.4 adds the ability to configure an email notification for sending alarms in regular time intervals whether or not an alarm is fired.

To enable a periodic alarm notification, follow these steps:

1. Go to **Menu > Configuration > System > Alarms Email**.
2. Click the **Add New** button.
3. In the **Enable Alarm Email Notifications** field, select **Yes** to enable sending email notifications for alarms.
4. In the **Enable Alarms Syslog Forwarding** field, select **Yes** to enable sending the syslog associated with an alarm. You can configure syslog destinations in the Syslog Destinations subtab.
5. In the **Minimum Severity to Send Email Notification** field, select the minimum severity level at which you want an alarm sent out. The recommended minimum severity level is **Major**.
6. The **Include Hadoop Platform Alarms** option allows you to include Hadoop platform alarms in the notifications. The recommended option is **Yes**.
7. In the **Recipient Email Address(es), Comma Separated** field, enter the email address to which the email is sent. You can enter multiple email addresses, separated by a comma.
8. In the **Send Notification...** field, select one of the **All Active Alarms** options to send information about all active alarms at the associated time interval. See Figure 9 for options.

Figure 9 *All Active Alarms Options*

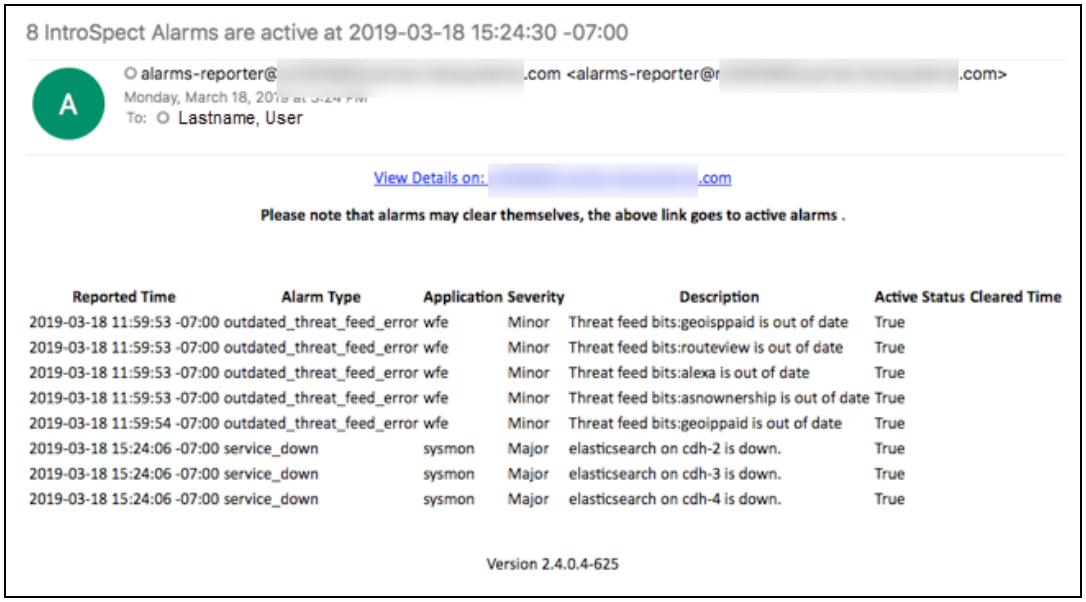


9. Click **Save**. If an option for **All Active Alarms** is selected:
   - An email or syslog is sent even when there are no active alarms in the system.
   - The notification email or syslog states that there are "0 IntroSpect alarm(s) active" in the system (see Figure 12).

Example Email Notifications

The following figures show various examples of periodic email notifications.

Figure 10 *Example Periodic Email Notification with Minor and Major Severity*



8 IntroSpect Alarms are active at 2019-03-18 15:24:30 -07:00

A

alarms-reporter@ .com <alarms-reporter@ .com>

Monday, March 18, 2019 at 3:24 PM

To: Lastname, User

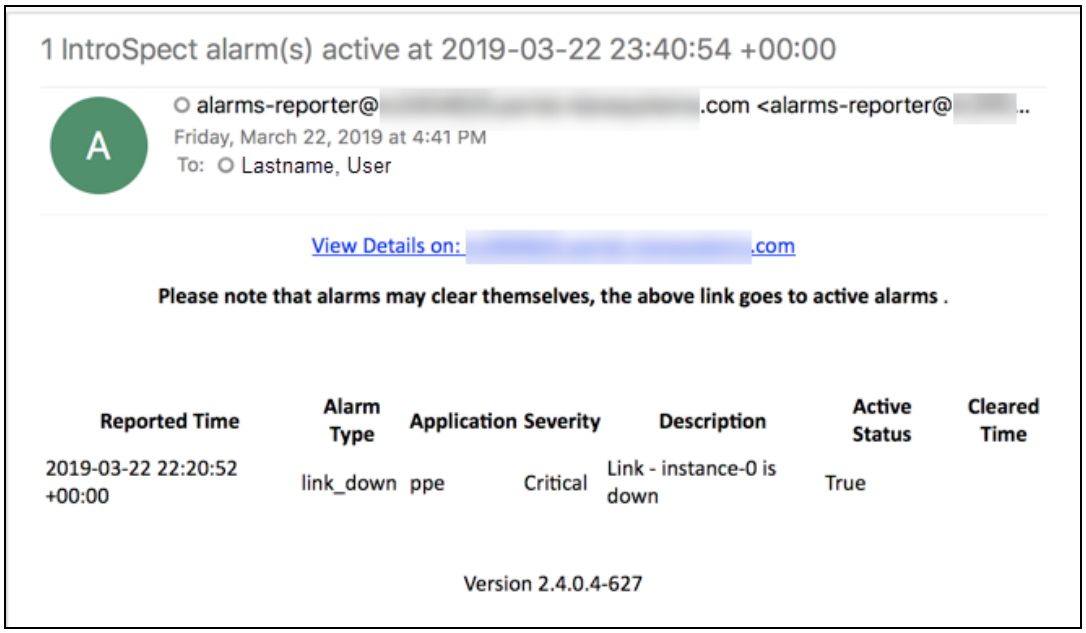
View Details on: .com

Please note that alarms may clear themselves, the above link goes to active alarms .

Reported Time	Alarm Type	Application	Severity	Description	Active Status	Cleared Time
2019-03-18 11:59:53 -07:00	outdated_threat_feed_error	wfe	Minor	Threat feed bits:geoisppaid is out of date	True	
2019-03-18 11:59:53 -07:00	outdated_threat_feed_error	wfe	Minor	Threat feed bits:routeview is out of date	True	
2019-03-18 11:59:53 -07:00	outdated_threat_feed_error	wfe	Minor	Threat feed bits:alexa is out of date	True	
2019-03-18 11:59:53 -07:00	outdated_threat_feed_error	wfe	Minor	Threat feed bits:asnownership is out of date	True	
2019-03-18 11:59:54 -07:00	outdated_threat_feed_error	wfe	Minor	Threat feed bits:geoippaid is out of date	True	
2019-03-18 15:24:06 -07:00	service_down	sysmon	Major	elasticsearch on cdh-2 is down.	True	
2019-03-18 15:24:06 -07:00	service_down	sysmon	Major	elasticsearch on cdh-3 is down.	True	
2019-03-18 15:24:06 -07:00	service_down	sysmon	Major	elasticsearch on cdh-4 is down.	True	

Version 2.4.0.4-625

Figure 11 *Example Periodic Email Notification with Critical Severity*



1 IntroSpect alarm(s) active at 2019-03-22 23:40:54 +00:00

A

alarms-reporter@ .com <alarms-reporter@ ..

Friday, March 22, 2019 at 4:41 PM

To: Lastname, User

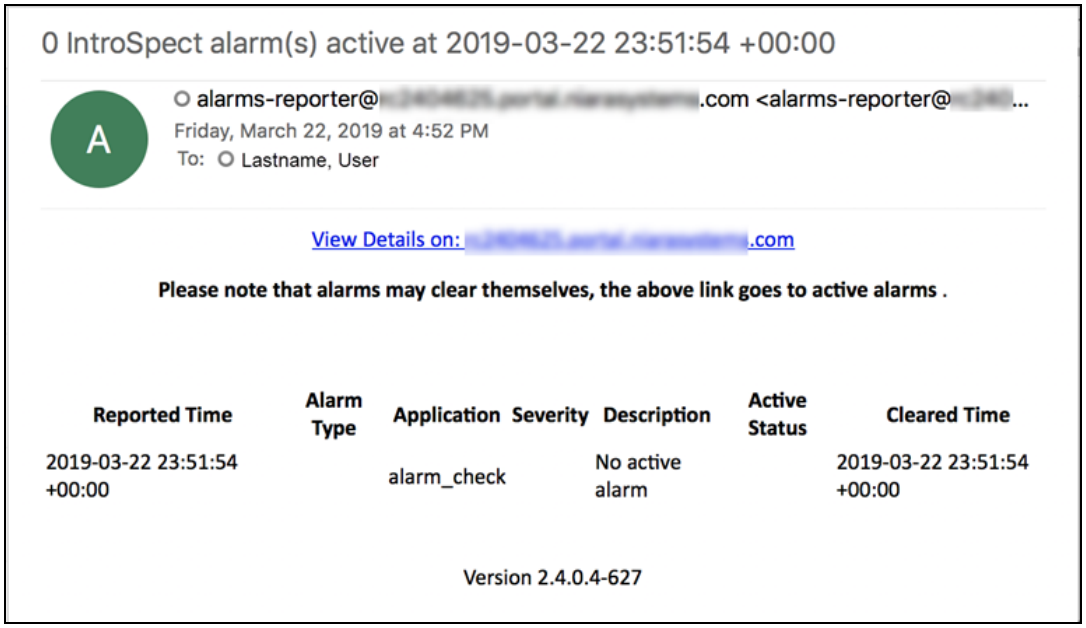
View Details on: .com

Please note that alarms may clear themselves, the above link goes to active alarms .

Reported Time	Alarm Type	Application	Severity	Description	Active Status	Cleared Time
2019-03-22 22:20:52 +00:00	link_down	ppe	Critical	Link - instance-0 is down	True	

Version 2.4.0.4-627

Figure 12 *Example Periodic Email Notification with No Active Alarms*



Backup Analyzer

The **Backup Analyzer** subtab within the **System** tab allows you to backup all the configuration from the primary Analyzer to a backup Disaster Recovery (DR) Analyzer. After setting it up, the information and settings configured in the Postgres database on the primary Analyzer are mirrored to the backup DR Analyzer.

NOTE

Configure this setting only after consultation with Tech Support.

Setting up a Backup Analyzer

To set up a backup Analyzer, follow these steps:

1. Go to **Menu > Configuration > System > Backup Analyzer > Add New**.
2. Use the **Primary Analyzer** options to indicate whether the current Analyzer is the primary.
3. Use the **Setup Backup Analyzer** option to setup a backup Analyzer and provide the information to access it.
   - Enter the access credentials for the backup Analyzer—enter a hostname, username, and password for the backup Analyzer.
   - Set the frequency for the backup activity.
4. Click **Save**.

ClearPass Servers

The **ClearPass Server** subtab is used to configure information sent to the ClearPass server.

This configuration enables Introspect to either quarantine devices as a result of an alert or elevated risk score associated with thise entities or restore them via ClearPass.

Configuring the ClearPass Server

Follow these steps to configure the ClearPass server to which the information is sent.

1. Go to **Menu > Configuration > System > ClearPass Servers**.
2. In the **ClearPass server host name or IP address** field,

3. Enter the **ClearPass server port** with which Analyzer will communicate. Port 443 is always used for this communication.
4. The **Client ID** is generated by ClearPass.
5. The **Client secret key** is generated by ClearPass. The grant type is: client_credentials.
6. Click **Save**.

DNS Servers

The **DNS Servers** configuration subtab is used to configure the DNS server IP addresses for instances where Analyzer needs to perform any DNS resolution.

You can configure two pre-populated DNS servers and also update them. These two servers are populated during the setup wizard when Analyzer is initially set up. After the initial setup, you can go to this configuration tab to update the configuration that was performed in the setup wizard.

Configuring DNS Server IP Addresses

Follow these steps to configure the DNS server IP addresses.

1. Go to **Menu > Configuration > System > DNS Servers**.
2. To add a new server, click **Add New**, enter the server IP address, and click **Save**.
3. To delete an existing server, click **Delete** below the server address.

Entity Email

The **Entity Email** subtab is used to configure notifications that are triggered when an entity's risk score changes. This configuration sends entity risk score changes through email or syslog to a third-party system such as Splunk or ArcSight. Whenever there is a change in the entity's risk score, a syslog containing the entity information and the risk score can be sent to the third-party system.

Configuring Entity Emails

Follow these steps to configure risk score change notification emails for entities.

1. Go to **Menu > Configuration > System > Entity Email > Add New.**
2. In the **Enable Entity Email Notifications** field, select an option to enable or disable sending email notifications for entities based on the criteria entered in the **Minimum Risk Score to Send Alert** field below.
3. In the **Enable Entity Syslog Forwarding** field, select an option to enable or disable sending the syslog associated with an entity Risk Score change when the notification condition (see Step 5) is met. You can configure syslog destinations in the Syslog Destinations subtab.
4. In the **Entity360 query, as typed in 'ENTITY360'** field, indicate the entities for which you want to send out this information.
   - Use the default query, ***.*** , when you want to send entity Risk Score information using syslog and email for all entities.
   - To limit the notifications to just a few entities, enter the query that you would type in on the Entity360 page. For instance, you can specify that you only want to send this information for specific entities, by username. Query: **user_name:johndoe**
5. In the **Minimum Risk Score to Send Alert** field, enter the minimum risk score for which to you want an entity notification sent out. The default value is 1. For instance, if you enter a value of 60, a syslog or email indication is sent out only for entities whose risk score is 60.
6. In the **Recipient Email Address(es), Comma Separated** field, enter the email address to which the email is sent. You can enter multiple email addresses separated by a comma.
7. In the **Include Entities...** drop down field, select an option:

- **All with risk score**—includes all entities with at least the minimum risk score defined in Step 5.
- **All for which risk score increased since last check**—includes all entities for which the risk score has increased since the last check.

8. In the **Send Notification...** field, select the frequency for the risk score email or syslog notifications. Your options include hourly, daily, or weekly notifications. The recommendation is to configure this as a **Daily Digest** so that you receive indications of the risk score changes on a daily basis.
9. In the **Time Zone in Notification Messages** field, select the time zone of the timestamp in the notification email.
   - All data in the backend is maintained normalized to UTC time.
   - If you select your time zone here, the timestamp in the notification emails that are sent out with the risk score changes are normalized to your time zone's timestamp.
   - If you have recipients in multiple time zones, it is best to leave the time zone in UTC. However, if you only have email recipients in one time zone, you should specify that particular time zone to make it easier to read.
10. Click **Save** to apply your changes.
11. You can click **Delete** to remove your entry.

External Apps

The **External Apps** configuration subtab is a demo prototype and soon to be deprecated. Please contact IntroSpect Support for details.

HTTP Server

The **HTTP Server** configuration subtab contains settings for X-Frame-Options.

When a client communicates with the IntroSpect web server using the UI, you have the option to insert an X-Frame-Options tag in the response from the Engine-X server. This option allows you to prevent click fraud by enforcing the server to only accept requests with the same origin.

Inserting X-Frame Options

Follow these steps to prevent other websites from embedding the IntroSpect UI:

1. In the **Prevent other websites from embedding this UI (with "X-Frame-Options: SAMEORIGIN")** field, the default and recommended option is **Yes**. When you click **Yes**, the following tag is inserted in the response from the Engine-X server:
   X-Frame-Options: SAMEORIGIN.
2. Click **Update**.

Interface Configuration

The **Interface Configuration** subtab allows you to change network interface settings that were previously configured during the setup wizard. Here you can configure the eth0 interface IP addresses and network interface information. These settings are typically configured in the setup wizard, but any subsequent updates can be performed through this tab.

IP addresses and network interfaces must only be changed through the UI at **Configuration > System > Interface Configuration**. The interface configuration is stored in the IntroSpect configuration database, as entered through in the UI.

If Packet Processor has already been bootstrapped to this Analyzer, updating the IP address will hinder the communication. Please contact IntroSpect Support before proceeding.

Do not use the generic CentOS method to update the interface IP address. The change is not permanent.

The administrator should be connected to the eth1 IP address in order to change the eth0 IP address or else risk losing connectivity to the cluster.

Some considerations include:

- On both Packet Processor and Analyzer, only the **eth0** interface is used for external communication. Use the **static** method for assigning IP addresses on all appliance-based systems. However, for Packet Processors running as VMs, use DHCP for dynamic assignment of IP addresses.
- Do not change the configuration of the other interfaces (**eth1**, **eth2**, and so on), unless directed by IntroSpect Support.
- When Packet Processor or Analyzer is relocated and the appliances moved to another subnet, refer to the procedure defined in the Quick Start Guides for Packet Processor or Analyzer. The appliances must be securely shut down before being moved. This task cannot be performed if the appliances become unreachable.
- Each interface supports a single IP address. There is no sub-interface and tagged port is not supported.

Make changes very carefully to avoid getting locked out of SSH and the UI. If you are locked out, follow the procedure described in the Quick Start Guides, visit the location where Analyzer is deployed, and connect a laptop or a crash cart to the **eth1** port on the **an-node**.

Interface Configuration Tab Fields

The following fields display information about the previously configured network interfaces. If needed, you can make updates to these settings here.

1. The **Name** field displays the network interface: **eth1** or **eth0**.
2. The **Enabled** field shows **Yes** by default indicating the interface which was previously configured. You can change these settings by selecting **Yes** to enable the interface or **No** to disable it. The recommendation is not to disable the interface, as you will lose connectivity to the box.
3. The **IPv4 Address/Length (or Mask)** field displays the IP address of the network interface .
4. The **Default IPv4 Router** field, displays the IP address of the default gateway router.
5. The **Addressing Method** field indicates whether the DHCP is **Static** or whether it is through a DHCP server. The preferred method of allocating IP address for Analyzer is **Static**.
6. If you make any changes here, click **Update** to save your settings.

LDAP Authentication

The **LDAP Authentication** subtab is accessed from **Menu > Configuration > System > LDAP Authentication**.

The **LDAP Authentication** subtab allows you to configure the system to use LDAP to authenticate user access to the Analyzer UI. LDAP authentication is an optional feature that allows authentication of the administrators of the system through LDAP as opposed to statically configured accounts in IntroSpect.

There are two parts to this configuration—LDAP Authentication and LDAP Role Mappings. LDAP authentication is currently supported only with Active Directory. Open LDAP or any other LDAP providers are not supported. Contact IntroSpect Support if this is required.

This feature applies only to UI access, and not SSH.

Basic LDAP Authentication

To configure the initial LDAP authentication, enter the information in the following fields (leaving the rest to default):

- **Priority**
- **Hostname**
- **Port**
- **Bind Distinguished Name/UPN**
- **User Query Distinguished Names**

The details of each field are as follows:

1. The **Enabled** field indicates whether LDAP authentication is enabled or disabled.
2. If you have two LDAP configurations, use the **Priority** field to designate a primary and a secondary LDAP server. Scroll down to see the entries for the second server.
3. In the **Hostname** field, enter the FQDN of the Active Directory server.
4. In the **Port** field, enter the port that is to be used. If it is SSL-enabled, use port 636.
5. In the **SSL** field, this indicates the LDAP mode, whether it is SSL or non-SSL.
6. In the **Bind Distinguished Name/UPN** field, enter the domain you wish to append to the username for authentication purposes. Consider setting to: %user%@your-domain.com
7. When you enter a username on the **Username** field of the Login screen of the UI, the system sends the username to the LDAP server, appended with the domain you enter here, for example, @arubanetworks.com. This gives you the flexibility to just enter the username and then have the system append the domain for authenticating the user with the LDAP server.
8. In the **Password** field, leave this entry to the default blank value in the basic mode.
9. The **User Query Distinguished Name** field is the LDAP tree location where this user's information is available to authenticate against. Consider setting to: CN=Users,DC=your-domain,DC=com
10. The **Common Name Identifier** is the field in the LDAP database that indicates what to authenticate against. This should never be changed. Typically, in all LDAP servers, **sAMAccountName** is the field to authenticate against.
11. The **Email Address Attribute** field is used to retrieve the email address from the LDAP records. When you authenticate for the first time, the system pulls the email address and populates it into the local LDAP database.

Advanced LDAP Authentication

The advanced authentication mechanism is useful in instances where you need to obtain the group membership of the user for which the authenticating user does not have access.

To obtain group membership information, you must configure a service account. The group membership information entered in the following fields is used to map to the role that the user will have when they log in to the system.

- **Group Query Distinguished Names**—Default root group OU in your directory service that is used to look up all groups to which the user belongs.
- **Group Membership Attribute**—Attribute used to look up group names, such as gidNumber.
- **Primary Group Attribute**—Attribute that contains your primary group value, such as primaryGroupId.

NOTE

For more details, and to implement this advanced authentication, contact IntroSpect Support.

LDAP Role Mappings

The settings in the **LDAP Role Mappings** tab are used to define roles with different access privileges onto your system. These roles are used by the LDAP authentication mechanism when obtaining LDAP group information for a user.

In this process, the user's LDAP group is used to map to the role for access to Analyzer. For example, if the user is a member of the **Domain Users** LDAP group, they are mapped to the **Superuser** privilege on the account.

Configuring LDAP Role Mapping

To configure the initial LDAP role mapping:

1. Go to **Menu > Configuration > System > LDAP Role Mappings > Add New**.
2. Configure the following fields:
   - **AD Group**— this can include any suitable AD group.
   - **User Role**—this is the IntroSpect role to which authenticated users are assigned**.** For details about the access privilege assigned to each role, please see User Accounts Tab Fields on page 88
3. Click **Save**.
4. To delete a user role, highlight the role and click **Delete**.

Mail Relay

The **Mail Relay** subtab is used to configure the mail server for sending out the Entity, Alarm, and Security Alert email notifications. When you enable these email notifications by selecting **Yes** in their respective **Enable** fields, you also need to configure the mail relay service.

It is highly recommended to configure a mail relay service. Mail relay should be configured on Analyzer. However, it is optional on Packet Processor.

The main function of the mail relay service on Analyzer is to send alarm notifications. Alarms from all Packet Processors are forwarded to Analyzer, which can be used as a single point to forward alarms. The exception is the **Analyzer Down** alarm, which is detected on Packet Processor.

NOTE

The **mail relay** service must only be changed through the UI from **Configuration > System > Mail Relay**. Do not use the generic CentOS method to update the mail relay name and address; this change is not permanent.

Mail relay configuration is a straightforward process. However, you will need to obtain mail server information, especially authentication requirements.

NOTE

One possible issue to watch for is the **Forced Sender Address** field. Many mail systems do not forward email unless the sender is part of specific domains. Consider entering a valid email address for your domain, such as **no-reply@your-domain**. By default, most of the notifications that can be enabled in the configuration use an auto-generated sender based on the domain found in the configured hostname, such as **alarms-reporter@acme.com**. This name can be overwritten by the configured **Forced Sender Address** field.

Configuring the Mail Relay Service

To configure the Mail Relay service:

1. Go to **Menu > Configuration > System > Mail Relay**.
2. In the **Server Name/Address** field, enter the server address of the mail server.

3. In the **Port** field, enter the communication port number. Two ports are provided, one of which is SSL-enabled and the other is not.
4. Select from the **Enabled** options to indicate whether this particular mail relay service is enabled.
5. The **Use Authentication** options indicate whether mail relay requires authentication (most enterprise mail servers require authentication).
6. In the **Authentication Type** field select the type of authentication: **NTLM** or **Plain**.
7. Enter the **User** (username) and **Password**. You may need to create a service account email address for this.
8. Enter the **Forced Sender Address**.
9. Select a **Use TLS** option to indicate whether or not you need to use TLS to authenticate.
10. Click **Update**.

Mail Relay Troubleshooting

Mail is sent using the standard Linux **postfix** facility with the associated configurations.

Debugging can be cumbersome because issues might occur with upstream systems. Once a mail relay service is configured, consider the following procedure:

1. Login to the system using SSH.
2. Use the command line to test. Enter the following command:
   ```
   echo "mail test" | mail -s "IntroSpect email test" <your email address>
   ```
3. An email is received after a few seconds.

Postfix logs are stored in **/var/log/maillog**. This log should contain an intelligible explanation if the email is not delivered.

The **Test** button in the **Configuration > System > Alarms Email** tab can also be used to expedite email configuration testing.

Netflow Port

The **Netflow Port** subtab shows the port through which Netflow is configured to be sent to IntroSpect Analyzer.

The **Port** field shows the default Netflow port which, for many Cisco switches, is 9996. If you need to use another port, change it here and click **Update**.

Netflow Subnet Filters

The **Netflow Subnet Filters** subtab is used to filter in the Netflow traffic only between the subnets listed here. This configuration only filters in internal-to-internal traffic.

These subnets are all RFC 1918 subnets, or internal subnets.

- To configure additional subnets, click the **Add New** button, enter the subnet address in the **Subnet prefix/length** field, and click **Save**.
- To edit a subnet address, change the information in the **Subnet prefix/length** field and click **Update**.
- To delete subnets (for instance if you want to pull in all traffic that is being sent via Netflow) select the subnet to remove and click **Delete**.

NTP Servers

The **NTP Servers** subtab is used to configure your NTP servers. Set up valid NTP servers in the UI at **Configuration > System > NTP servers** for Packet Processor and Analyzer.

IntroSpect systems are shipped with the default CentOS NTP servers configured. If those are reachable, no further actions are required.

However, you can update these servers. To update the servers listed here, you must delete an existing server before you can add a new NTP server.

Some considerations include:

- Improperly synchronized time makes system issues difficult to review and debug.
- An alarm is raised if NTP is not synchronized.
- On Analyzer, time synchronization between all the nodes is essential for the Hadoop platform to function. The an-node time is synchronized according to the configuration. It also act as an NTP server for the compute nodes, ensuring that all Analyzer nodes have the same time, regardless of whether the an-node itself is properly synchronized.

Security Alerts Email

The **Security Alerts Email** subtab is used to configure notifications for security alerts that are generated in the system as a result of IntroSpect analytics. These alerts can be configured to be sent by email or syslog to a third-party device.

Configuring Security Alert Emails

Follow these steps to configure security alert notification emails.

1. Go to **Menu > Configuration > System > Security Alerts Email > Add New.**
2. In the **Enable Alert Email Notifications** field, select an option to enable or disable sending email notifications.
3. In the **Enable Alert Syslog Forwarding** field, select an option to enable or disable sending the syslog associated with an alert. You can configure syslog destinations in the Syslog Destinations subtab.
4. In the **CEF Syslog Format** field, select an option to enable or disable sending the syslog in Common Event Format (CEF).
5. In the **Alert query, as typed in 'ALERTS'** field, enter the query for the alerts you want to be sent out.
   - Use the default query, ***.*** , when you want to send notifications using syslog and email for all alerts.
   - To limit the notifications to just a few alerts, enter the query that you would type on the **Alerts** page. For instance, you can change it to only send alerts that are for a particular user account.
     Query: **user_name:john***
6. In the **Minimum Severity to Send Alert** field, enter the minimum severity to send out the alert. The default value is 0. For instance, if you enter a value of 60, a syslog or email indication is sent out only for alerts with a minimum severity of 60.
7. In the **Minimum Confidence to Send Alert** field, enter the minimum confidence to send out the alert. The default value is 0. For instance, if you enter a value of 60, a syslog or email indication is sent out only for alerts with a minimum confidence of 60.
8. In the **Recipient Email Address(es), Comma Separated** field, enter the email address to which the email is sent. You can enter multiple email addresses separated by a comma.
9. In the **Send Notification...** field, select the frequency for the alert email or syslog notifications. Your options include: as alerts are produced, or as a digest every 4 or 8 hours, or daily or weekly digests. The recommendation is to configure this as a **Daily Digest** so that you get one email a day with all the security alerts that have been generated in the system for your security analysts to investigate.
10. In the **Time Zone in Notification Messages** field, select the time zone of the timestamp in the notification email.
    - All data in the backend is maintained normalized to UTC time.

- If you select your time zone here, the timestamp in the notification emails that are sent out are normalized to your time zone's timestamp.
- If you have recipients in multiple time zones, it is best to leave the time zone in UTC. However, if you only have email recipients in one time zone, you should specify that particular time zone to make it easier to read.

11. Click **Save** to apply your changes. To discard your changes, click **Delete**.

Syslog Destinations

The **Syslog Destinations** subtab is used in conjunction with the **Entity Email**, **Alarms Email**, or the **Security Alerts Email** settings to configure a destination to which you want to send syslogs. If syslog forwarding is enabled in those tabs, you need to configure a destination here.

Configuring a Syslog Destination

To configure a syslog destination, follow these steps:

1. Go to **Menu > Configuration > System > Syslog Destination > Add New**.
2. In the **Syslog Destination** field, select the syslog destination (IP or host).
3. In the **Port** field, enter the port for sending the syslog. The typical syslog port is port 514.
4. In the **Protocol** field, select the protocol you wish to use—UDP or TCP.
5. In the **Facility** dropdown field, select the facility that you want to use—options range from Local0 to Local7.
6. In the **Send UTF-8 BOM** field, you can choose to send the syslog as UTF-8 byte order mark (BOM).
7. In the **TCP Framing** dropdown, select a framing option: **Traditional (Newline)** or **Octet-Counted**.
8. In the **Enabled** field, select **Yes** to enable the destination settings or **No** to disable them.
9. Click **Save**.
10. Repeat these steps for each destination that you need to configure.

Time Zone

The **Time Zone** subtab is used to configure the time zone on the system and the user interface. The system time zone is configured during the setup wizard when Analyzer is set up. You can override the configuration here, if needed.

Considerations include:

- It is required to configure the time zone to your local time zone.
- The time zone setting sets the Linux time zone to the configured value with all the usual Linux effects.
- The time zone is used for Behavioral Analytics.

Configuring the Time Zone

To configure the time zone:

1. Go to **Menu > Configuration > System > Time Zone**.
2. In the **Time Zone** field, select your local time zone from the drop down list. This is the system time zone used for Analytics.
3. In the **User Interface Time Zone** field, select an option to set the time zone displayed in the UI:
   - **UTC**
   - **Browser Time Zone** (Recommended)
4. Click **Update** to apply your changes.

Web Proxy

The **Web Proxy** subtab allows you to configure a proxy for Internet access, if present in your network environment. For instance, this is useful for on-line software upgrade from the Aruba software repository on the internet or to update IOC Threat feed. You can configure a proxy at **Menu> Configuration > System > Web Proxy**.

Some considerations include:

- Authenticated and non-authenticated proxies are supported.
- Automatic proxy discovery and automatic proxy configuration are not supported.
- Internet access is required for several analytics features on Analyzer, including update of Alexa lists, IOCs, and geo-location databases. Internet access to IntroSpect repositories is the fastest way to perform software updates.
- This proxy setting is used by tasks requiring Internet access.

Configuring a Web Proxy

To configure a web proxy server, follow these steps:

1. Go to **Menu > Configuration > System > Web Proxy**.
2. Enter the **Web Proxy Server** name.
3. If authentication is required for the proxy server, enter the **User Name** and **Password**.
4. Enter a **Port Number**.
5. In the **Enabled** field, you can
   - Select **Yes** to enable the proxy and route all internet access through the proxy, or
   - Select **No** to disable it.

Configuration—User Accounts

The **User Accounts** tab on the **Configuration** page allows you to configure or manage users on the system.

The following table describes the fields on the **User Accounts** tab.

Table 26: *User Accounts Tab Fields*

Field	Description
Username	Username of the user account.
Role	Role assigned to the user. Options are: ■ **Superuser**—By default the IntroSpect system comes with a user **admin** role with superuser privilege. This role allows a user to perform every operation that is available from the UI. Users with this role can look at all the data, alerts, logs, setup, configure and manage the system. They have permission to every action available during alert investigation. ■ **Senior Analyst**—This role is primarily for users who investigate alerts and tune analytics. Users with this role can also create, edit or delete rules. They are not allowed to modify system configuration or management. ■ **Analyst**—This role is primarily for users who are allowed to view data and investigate alerts. Users with this role are not allowed to modify system configuration or management. They are not allowed to manage rules or change any analytics configuration. ■ **Read-only Analyst**—This role is primarily for users who view data and investigate alerts. Users with this role are not allowed to modify system configuration or management. They cannot manage rules or change any analytics configuration. They cannot modify alerts or alert investigations, edit comments on entities, create watchlists or assign entities to them, or save search queries. ■ **Obfuscated Analyst**—This role is primarily for users who are not allowed to view personally identifiable information (PII) for any user. For instance, this role sees user Jane Doe as a randomized set of characters, such as *aaxxbbee*, instead of *Jane Doe* and cannot correlate this randomized set of characters to Jane Doe.
2FA Enabled	Whether Two Factor Authentication (2FA) is Enabled or Disabled. Two Factor Authentication (2FA) is a two step verification that provides an extra layer of security.
LDAP Enabled	Whether LDAP authentication is Enabled or Disabled.
Status	Status of the user account: Enabled or Disabled.
Last Login	Date and Time of the last login for the user account.
Created	Date and Time the user account was created.

Adding a New User

To add a new user, follow these steps:

1. Go to **Menu > Configuration > User Accounts**.
2. Click the **Add Use**r icon at the top of the page.
3. Provide the following details:
   - **Username**
   - **E-mail**
   - **Password** and confirmation
4. You can enter a custom **Default Start and End Date** which sets the default time range for the user when accessing the UI. This is unrelated to the time range where this account is enabled or disabled.

   The default date range shows data for the past week. To set a custom date range, select the dates in the time range picker. Future logins will use the custom date range instead of the default.
5. In the **Status** field, enable or disable the account status.
6. From the **Role** drop-down field, select the user's role. The options include:
   - **Superuser**

- **Senior Analyst**
- **Analyst**
- **Read-only Analyst**
- **Obfuscated Analyst**

7. Click **Save**.

Editing User Account Settings

To update any of the settings for a user account, follow these steps:

1. Go to **Menu > Configuration > User Accounts**.
2. Scroll or filter by username to locate the user you wish to edit.
3. Click on the **Edit** icon in the **Username** column. The Edit options are displayed.
4. In the **Edit User** tab, edit the following settings as you need:
   - **Username**
   - **E-Mail**
   - **Password** and confirmation
5. In the **Status** field, you can enable or disable the account status.
6. From the **Role** drop-down field, select the user's role. The options include:
   - **Superuser**
   - **Senior Analyst**
   - **Analyst**
   - **Read-only Analyst**
   - **Obfuscated Analyst**
7. In the **2FA Enabled** field, you can choose to enable or disable the user 's 2FA permissions. Two Factor Authentication (2FA) is a two step verification that provides an extra layer of security.
8. In the **Settings** tab, you can change the **Default Start and End Date** range. Your options include:
   - The **Default** time range (one week)
   - **Custom dates** (select a range using the time picker in each field).
9. Click **Save**.

Editing Multiple Users

You can enable, disable, or delete mutiple users at the same time. To edit one or more user accounts, follow these steps:

1. Go to **Menu > Configuration > User Accounts**.
2. Click in the checkbox column to select the row for the user you wish to edit. You can select multiple users if you wish to apply the same changes to all of them.
3. In the **Bulk Action** card that appears at the bottom of the browser window, click the **Click to set an action** text.
4. In the **User List Actions...** pop-up box, select an option: **Enable**, **Disable** or **Delete User**.
5. Click the **go** arrow. A confirmation pop-up window opens.
6. Click **OK** to apply your changes or **Cancel** to discard them.

Obfuscating Personally Identifiable Information (PII)

Configuration—Cluster

From the **Cluster** tab on the **Configuration** page you can view information, configure and manage the cluster. This tab contains the following sub-tabs:

- Initial Install
- Software Update
- Cluster Start/Stop
- Data Ingestion Start/Stop

Initial Install

The fields on the **Initial Install** tab are only available when the system is initially set up. This tab is primarily used to configure the Hadoop platform on the system during initial setup, and is not available for subsequent use.

Software Update

The **Software Update** tab provides the ability to update the system.

To upgrade the software version on Analyzer:

1. Go to **Menu > Configuration > Software Update**.
2. In the **Version Number or Upload Image** field, you have two options for upgrading:
   - Enter the software version to which you want to upgrade.
   - Click the **Choose Image** button to browse to a local file on the system (an image file that was previously downloaded onto the system).
3. Click **Upgrade Now**.

Cluster Start/Stop

The **Cluster Start/Stop** functionality has means to start or stop the entire Analyzer cluster.

Hover over the question mark icon to see details for each option. The options include:

- **Restart Cluster**—restarts all the nodes on the system, including the an-node and the compute nodes.
  - Restarts all cluster services, including Hadoop.
  - Takes several minutes.
- **Restart Cluster (Safe Mode)**—shuts down everything in a safe manner. This is the preferred approach.
  - Restarts all cluster services, including Hadoop.
  - Removes data not fully ingested.
  - Repairs some issues.
  - Takes several minutes.
- **Stop and Reboot**—stops all the running processes on the system safely and reboots the entire cluster.
  - Stops all services safely, including Hadoop.
  - Reboots cluster nodes.
  - Click **Restart Cluster** after reboot.

- **Stop and Power Off**—safely shuts down everything and powers off all the nodes. Useful when you need to move or service the nodes.
  - Stops all services safely, including Hadoop.
  - Turns off cluster nodes.
  - Click **Restart Cluster** after turning on.

Data Ingestion Start/Stop

The **Data Ingestion Start/Stop** buttons allow you to start or stop the ETL processes which run on the system. The ETL processes ingest the data and load it into the system's databases. The options include:

- **Start Data Ingestion**—restarts previously stopped data ingestion.
- **Stop Data Ingestion**—shuts down data ingestion services for sensors and all sources. New data is not available in the cluster except for a small Analyzer buffer.
- **Restart Data Ingestion**—restarts the core data ingestion services.

Before performing any of these operations, please ensure you know the implications of starting or stopping data ingestion or the cluster, or doing an upgrade as all the operations in this tab impact the availability of the system during their operation.

Configuration—Analytics

The **Analytics** tab is accessed from **Menu > Configuration > Analytics**. The **Analytics** tab provides configuration options to manage analytics on the IntroSpect system.

The **Analytics** tab contains the following subtabs:

- DNS Server IPs
- Web Proxy IPs
- Correlator Config
- Sensitive Email Subject/Attachment Keywords
- User Correlation Config
- Domain Controller Configuration
- IP Subnet Range Configuration
- Account Attribute List
- Entity Black/White Lists
- Config Subnet
- Workflow Configuration

The details of this configuration will be available in a future document update.

Domain Controller Configuration

The **Domain Controller Configuration** subtab is accessed from **Menu > Configuration > Analytics > Domain Controller Configuration**.

This configuration enables the analytics to identify AD logs coming from the listed domain controllers. You can list specific domain controllers either by their exact host or computer name or patterns of names on this tab.

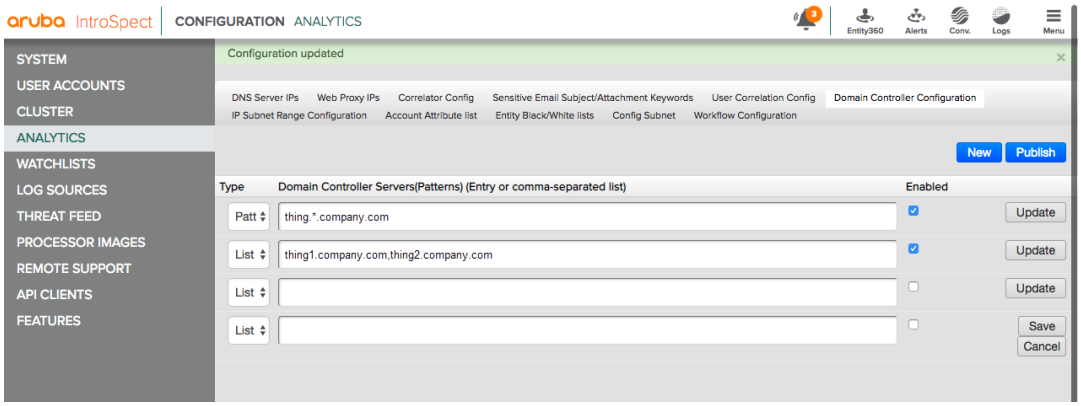
NOTE

If you are not receiving Windows AD security event logs from endpoints, there is no need to configure domain controllers as described in this section. By default, it is assumed that Windows AD security Event logs are received from the domain controller. You need to identify the complete list of domain controllers in this page only when you are processing Windows AD security event logs from both endpoints and domain controllers.

To add a domain controller:

1. Go to **Menu > Configuration > Analytics > Domain Controller Configuration**.

Figure 13 *Analytics Domain Controller Configuration Subtab*



2. Click **New.** Enter the following information for the specific domain controller in the fields.

Table 27: *Domain Controller Configuration Fields*

Field	Description
Type	**List**: Enter the exact name (host name or computer name) of the domain controller. For example: **thing1.company.com, thing2.company.com**
	Pattern: Enter a pattern to identify domain controllers with similar names. You can use wildcard characters in regex pattern match syntax. For example: **thing.*.company.com**
Enable	Select this option to enable the associated configuration.
Update	Click to apply the associated configuration in the system.
Save	Click to save any configuration. This does not apply or update the associated configuration.
Publish	Click to publish any changes using this configuration in the system.

3. Click **Publish**.

Configuration—Watchlists

The **Watchlists** tab allows you to create new watchlists or edit existing watchlists that you might have created from other pages in the UI such as the **Home** page.

A watchlist is a select list of entities that you wish to monitor closely. You can use watchlists that you create as facets to include or exclude entities from the results of the queries displayed on the **Alerts** and **Conversations** pages.

The following fields are available on this tab.

Table 28: *Watchlist Tab Fields*

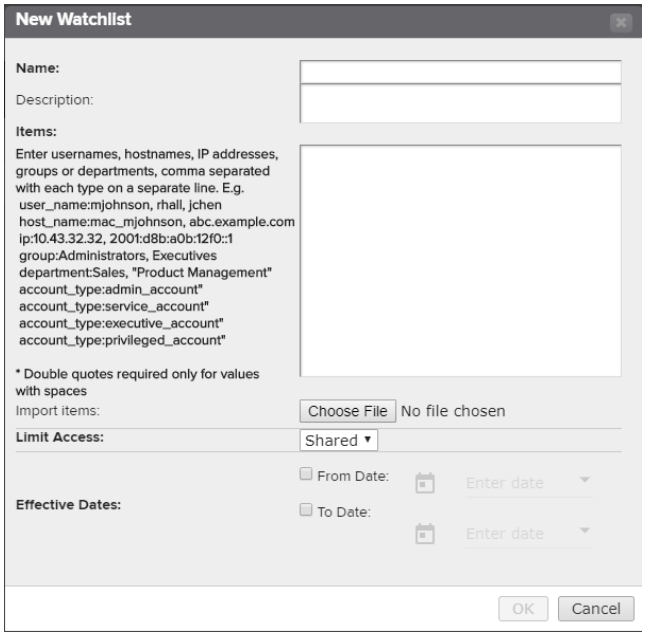
Field	Description
Checkmark	Select this icon to highlight a watchlist row for further edits.
Name	The watchlist name.
Item Count	Indicates the number of entities contained in the watchlist.
Description	Provides the description entered when the watchlist was created.
Private	Indicates the access limits set on this watchlist: they can be one of the following types: ■ **Private**—limited to your user account ■ **Public** (Shared)—shared with all other users
Effective Duration	Indicates the time period during which the watchlist is in effect.

Adding a New Watchlist

To add a new watchlist:

1. Go to **Menu > Configuration > Watchlists**.
2. Click the **New Watchlist** icon at the top of the page. The **New Watchlist** window opens.

Figure 14 *New Watchlist Dialog*



3. In the **Name** field, enter a name for the watchlist.
4. In the **Description** field, enter a description for the watchlist.
5. In the **Items** list, you can add items to the watchlist now or later. When you are ready to add items, use either of the following options:
   - Manually enter the accounts that you want to be added to this particular watchlist.
   - Import items using a file on your local laptop.
6. As you enter usernames, hostnames, IP addresses, groups, or departments, ensure that:
   - They are comma-separated with each type on a separate line.
   - You use double quotes when entering values with spaces.

   Examples:

- user_name:mjohnson, rhall, jchen
- host_name:mac_mjohnson, abc.example.com
- ip:10.43.32.32, 2001:d8b:a0b:12f0::1
- group:Administrators, Executives
- department:Sales, "Product Management"
- account_type:admin_account"
- account_type:service_account"
- account_type:executive_account"
- account_type:privileged_account"

7. In the Limit Access drop-down field, select from the following:
   - **Shared**—select this option to share this watchlist with other users.
   - **Private**—select this option if this watchlist is just meant to be for your user account.
8. In the **Effective Date** field, enter the date range during which the watchlist will be in effect.
9. Click **OK** to save your changes.

Editing a Watchlist

To edit an existing watchlist:

1. Go to **Menu > Configuration > Watchlists**.
2. Scroll or filter by **Name** to locate the watchlist you wish to edit.
3. Click on the **Edit** icon in the **Name** column. The **Edit Watchlist** window appears.
4. Edit any of the information for the watchlist.
5. Click **OK** to save your changes.

Configuration—Log Sources

The **Log Sources** tab is accessed from **Menu > Configuration > Log Sources**.

The details of this configuration will be available in a future document update.

Configuration—Threat Feed

The **Threat Feed** tab allows you to configure a threat feed source from a third-party vendor such as ThreatStream or Soltra. This feature is available in the Advanced Edition of IntroSpect.

A threat feed is a collection of data (including IPs and domains of malware, botnets, trojans, and others) which provides users with constantly updated information about potential or current threats to an organization's security. Third party vendors provide APIs which can be used to download their threat feed data.

By matching the network conversations against the feed data which the Analyzer node downloads from the feed servers, IntroSpect detects instances where machines in your organization might be communicating with these bad domains and IPs and become infected by the malware. IntroSpect looks for destination IP, destination host, or URL (including host and path) matches.

Please contact IntroSpect Support and use the third-party vendor provided credentials to configure new threat feeds.

Adding a New Threat Source

To add a new threat feed source to the system:

1. Go to **Menu > Configuration > Threat Feed**.
2. Click **New Threat Source**. The **New Threat Feed** dialog opens.
3. Select a **Vendor** from the dropdown. IntroSpect supports ThreatStream and Soltra. The following fields are then pre-populated with the options that IntroSpect supports:
   - **Category**—Threat Intelligence
   - **Format**—STIX/TAXII (STIX is an industry standard format for sharing threat intelligence data using the TAXII protocol.)
4. In the **Source** drop-down field, select **New Source**.
5. The **Source** dialog opens. Enter the vendor-provided credentials in the following fields to fetch the data from the feed server.
   - Hostname
   - Port
   - SSL—Enabled, STARTTLS, Disabled
   - Username
   - Password
   - Discovery Path
   - Label
   - Connect Using—Clear Text, HTTPS, Two-way SSL Handshake
6. In the **Feeds** text field, enter the feed names to be downloaded from the server. To configure multiple feeds, use a comma-separated list in the text field.
7. Click **Test** to test the configuration. The **Test Successful** message appears in the **New Threat Feed** dialog.
8. Click **OK** in the **New Threat Feed** dialog to configure the feed. The backend workflow then begins fetching the data from the feed server.

Editing an Existing Threat Feed Source

To edit an existing threat feed source:

1. Go to **Menu > Configuration > Threat Feed**.
2. Existing threat feeds are listed by **Vendor** and **Source**.
3. Click on an existing threat feed to edit it. The **Edit Threat Feed** window opens displaying the existing configuration for the selected threat feed.
4. Click on a **Source** to edit it. The **Source** dialog opens.
5. Edit the **Source** configuration using the vendor-provided credentials and click **OK**.
6. In the **Edit Threat Feed** dialog, in the **Feeds** text field, edit or enter the feed names to be downloaded from the server. To configure multiple feeds, use a comma-separated list in the text field.
7. Click **Test** to test the configuration.
8. The **Test Successful** message appears in the **Edit Threat Feed** dialog.
9. Click **OK** in the **Edit Threat Feed** dialog to configure the feed. The backend workflow then begins fetching the data from the feed server.

Configuration—Remote Support

The Remote Support tab provides the ability for IntroSpect Support to gain access into your cluster.

Contact IntroSpect Tech Support before enabling remote tunnel support.

Enabling a Remote Support Connection

To give Tech Support access to your Analyzer prompt, both the UI as well as the Linux shell:

1. Go to **Menu > Configuration > Remote Support**.
2. Click the **Enable Remote Support** button to create an SSL tunnel to an AWS instance in the cloud.
3. Set the duration for the remote support tunnel. Options are:
   - **Indefinitely**—Use this option to keep the support tunnel open at all times, allowing Aruba Tech Support to access your system at any point in time.
   - **For next_hours**—Use this option to set a time window where access is limited to a certain number of hours.
4. Once you enable the tunnel, provide the Public SSH key to Aruba Tech Support to gain access to Analyzer.

Optional Remote Support Configuration

You have the option to change the proxy's hostname or SSH port if needed.

1. Click on **Advanced** and configure the following fields:
   - **Proxy's Hostname**—This is the hostname of the AWS instance where Aruba Tech Support is hosted and where the tunnel is terminated.
   - **Proxy's SSH Port**—Enter the Proxy SSH Port that is being used. Port 443 is usually open on most networks and would be the ideal port.
2. Click **Submit**.
3. The fields below the **Submit** button provide you with additional information such as the status of the tunnel, and whether the tunnel is up for both SSH access to the Linux shell and the UI access to Analyzer.

Configuration—API Clients

The **API Clients** tab allows you to set up external access to alerts and conversations for various business needs such as generating reports, populating a Business Intelligence dashboard, or providing input to a security orchestration application such as Phantom.

On this tab, you can create API Clients which allow external applications to query information from IntroSpect Analyzer using a REST API. The system uses OAuth for access control. Currently, the following endpoints are available:

- Alerts
- Conversations

Setting Up External Access to Alerts and Conversations

To set up external access, follow these steps:

1. Consult the standard Swagger based REST API provided for accessing the documentation. The URL is: https://<IP or hostname of Analyzer>:8443/api-specs/
2. Within the IntroSpect UI, create a new Client ID and Secret (required to use the REST API). See Creating a New API Client

3. For guidance with this step, view the Sample Implementation using Python code which is available at the Aruba Security GitHub.

Creating a New API Client

To create a new API client:

1. Go to **Menu > Configuration > API Clients**.
2. Click the **New Client** icon at the top of the page. The **New Client** window opens.
3. In the **Name** field, enter a name for the client.
4. In the **Role** dropdown field, select the access privilege for the client.
5. Click **OK**.

This process creates a Client ID/Secret pair which can be used by third-party applications to generate an OAuth token for follow-on queries to Analyzer without re-authentication.

When a new OAuth token is generated for a Client ID/Secret pair, the previously generated token is invalidated. The unique Client ID/Secret pair should be used for each application.

Sample Implementation

A sample implementation of a client application (written in Python) can be found at the Aruba Security GitHub: https://github.com/aruba/introspect-api-python-snippets

Configuration—Features

The **Features** tab provides access to the Basic or Advanced editions of IntroSpect Analyzer.

Only access the edition to which you are licensed. Switching between modes can result in a loss of data.

- **Advanced Features**—provides access to the Advanced edition of IntroSpect which includes features such as the **Conversation** page, threat hunting, the **Log** page, and the **Rules** page.
- **Debug Mode**—provides Tech Support with additional debugging capabilities on the system. This feature is reserved exclusively for use by Tech Support.

Configuration—Processor Images

The **Processor Images** tab allows you to upload an image file for upgrading the Packet Processor code version from the Analyzer UI.

Please contact IntroSpect Support before you begin. You will need to download the Packet Processor image file from the location provided by IntroSpect Support.

Upgrading the Packet Processor Code Version

To upgrade the Packet Processor code version from the Analyzer UI:

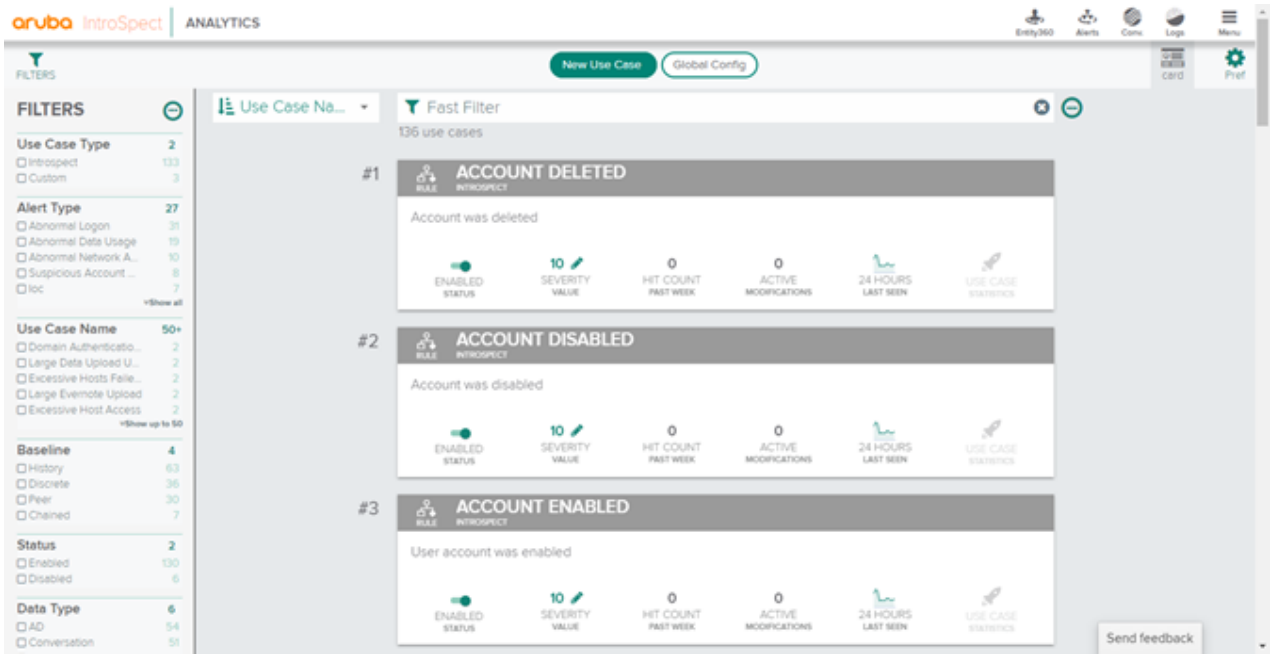
1. Download the Packet Processor image file from the location provided by IntroSpect Support.
2. Go to **Menu > Configuration > Processor Images**.
3. Click **Upload Image** at the top of the page.
4. Browse to the location of the saved Packet Processor image file, select it, and click **OK**.
5. Next, navigate to **Menu > System Status > Processors**.
6. Select one or more Packet Processors.

7. In the **BULK ACTION** card that appears at the bottom of the browser window, click the **Click to set an action...** text.
8. In the **Upgrade** popup, select the **Upgrade from Analyzer** option.
9. Click the **go** arrow. A confirmation pop-up window opens.
10. Click **OK** to start the upgrade or **Cancel** to cancel the upgrade.

This chapter describes the information available from the main **Analytics** page in the Analyzer UI. You can access this page from **Menu > Analytics**.

The **Analytics** page provides a view of the various use cases available in the system. These use cases are presented in a card format where each card represents a single use case. From this page you can access the settings on the analytics, create and modify existing use cases, and configure global parameters that apply across all the analytics. The following topics are available:

Figure 15 *Analytics Page*



Use Cases

A use case is an analytics configuration for analyzing an entity's behavior within a certain context such as "bytes uploaded to an external server" and so on. These defined contextual behaviors are called use cases and are used to trigger alerts when the conditions specified in them are met.

Use cases are identified by their names which consist of descriptive terms for various types of entity behavior that can occur in the network. For example: **Large Drobox Upload**, **Multiple Suspicious Command Execution**, and so on. Use cases can be classified as behavioral (learned) or rule-based depending on the logic they employ.

- **Behavioral**—A behavioral use case analyzes an entity's behavior in comparison with its own historical data, or that of its peers. Entity behaviors are learned by the system over time forming a baseline. Alerts are triggered by anomalies detected against this baseline data, in the context of the use case, and can involve multiple records. See Figure 16.
- **Rule-based**—A rule-based use case employs rules to filter out data that is considered for the use case in order to create alerts based on that data. Alerts are triggered if one or more records match the use case settings. See Figure 17.

Figure 16 *Behavioral Use Case*

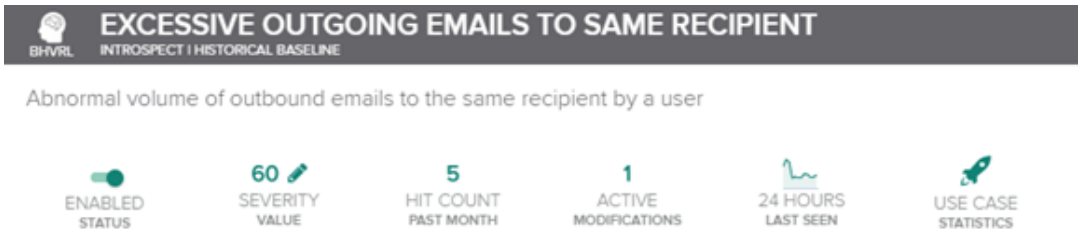
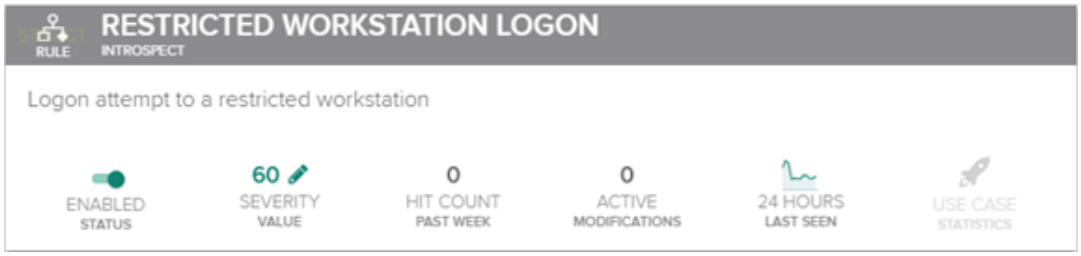


Figure 17 *Rule-based Use Case*



Use Case Types

IntroSpect identifies two basic types of use cases based on their origination. The **Use Case Type** category is available as an option from the **Filters** pane on the **Analytics** page.

- **IntroSpect**—These are pre-defined use cases which are shipped with the product.
- **Custom**—These include any user-defined use cases.

Use Case Card Fields

Use cases are displayed as cards showing detailed information. See Figure 18 for the various types of information presented on each card.

Figure 18 *Use Case Card Fields*

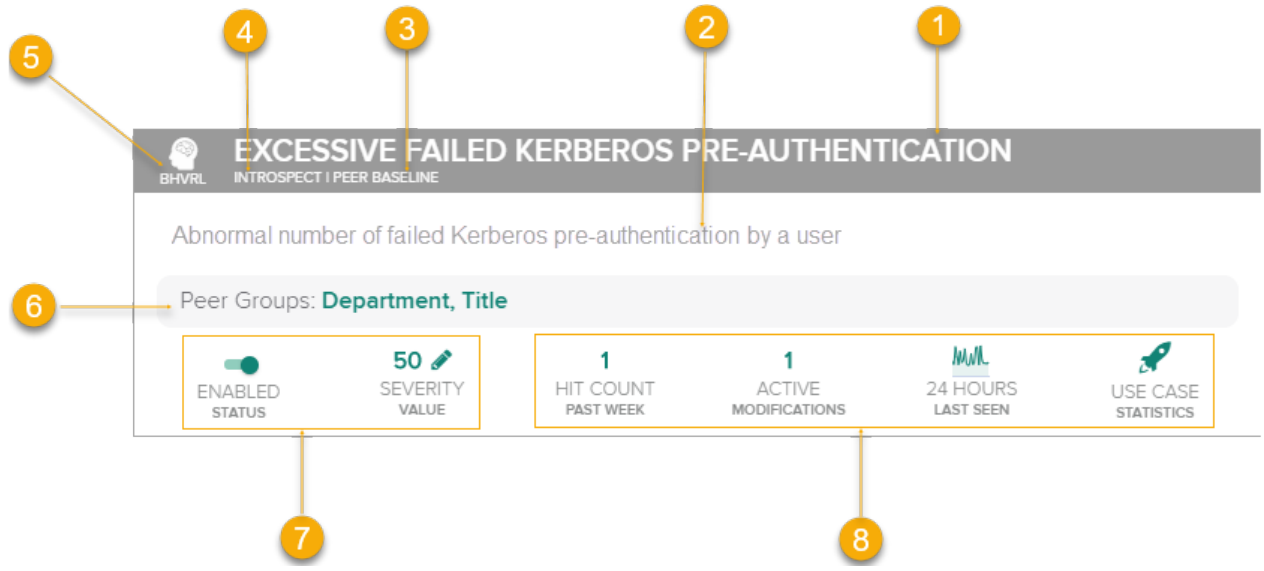


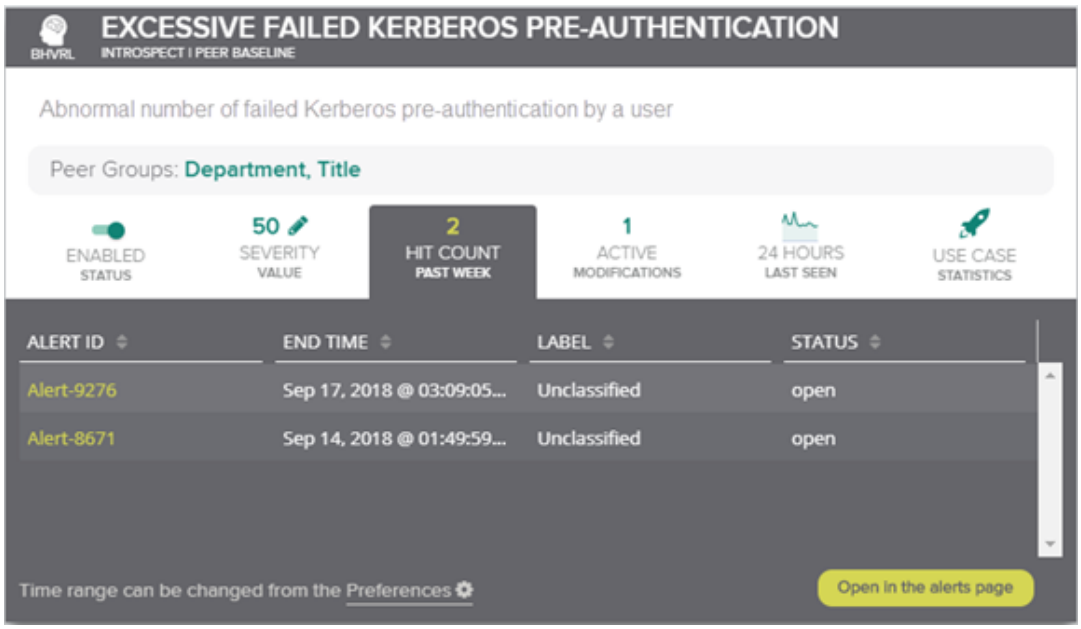
Table 29: *Use Case Card Field Details*

Legend	Description
1	The unique use case name.
2	A brief description of the use case.
3	The baseline data considered for the entity associated with the use case. There are two options that the data for the entity is compared against: Historical or Peer. ■ Historical: The entity's own history ■ Peer: The entity's Peer groups. These can be global (Enterprise) or specific (Organization Unit, Department, Title, Manager, Device Category, Account Type)
4	The use case type based on use case origin: predefined **Introspect** use cases or user-defined **Custom** use cases.
5	The use case classification based on the subset of the data type considered: Rule-based or Behavioral.
6	The peer group or groups used in the context of the use case.
7	These fields can be edited inline for the use case: ■ **Status**: toggle to enable or disable the use case ■ **Severity**: value considered for the entity risk score calculation
8	These tabs provide further information regarding the use case. Click each tab to display additional information. ■ Hit Count ■ Modifications ■ Last Seen ■ Statistics

Use Case Hit Count Tab

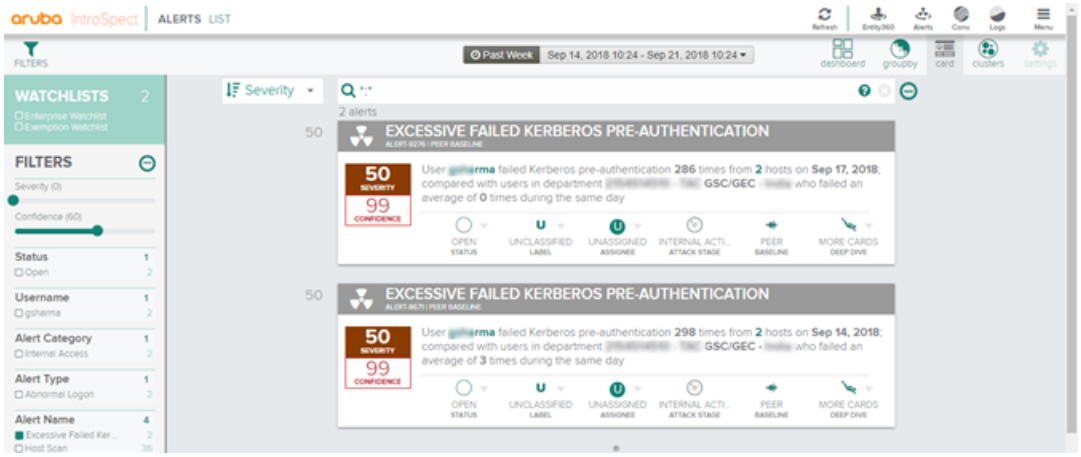
Figure 19 shows the **Hit Count** tab on the use case card. This tab displays the number of alerts that were fired for the use case in the selected time period. In this example, the time period is the past week.

Figure 19 *Hit Count Tab*



You can click the **Open in the alerts page** button to view the alerts on the **Alerts** page. See Figure 20.

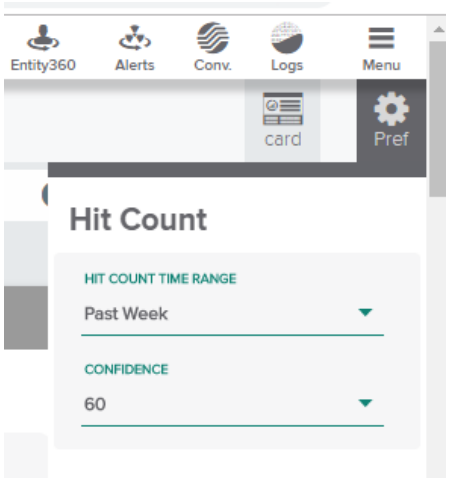
Figure 20 *Hit Count Alerts Opened in the Alerts Page*



You can also change the **Hit Count Time Range** and **Confidence** level for viewing use cases from the **Preferences** settings. See Figure 21.

- Time range options include **Today**, **Yesterday**, **Past Week**, and **Past Month**.
- Confidence level options range from 0-100 in increments of 10. By changing this value, you can set the confidence range for the display of alerts that exceed the entered confidence number.

Figure 21 *Hit Count Preferences Settings*

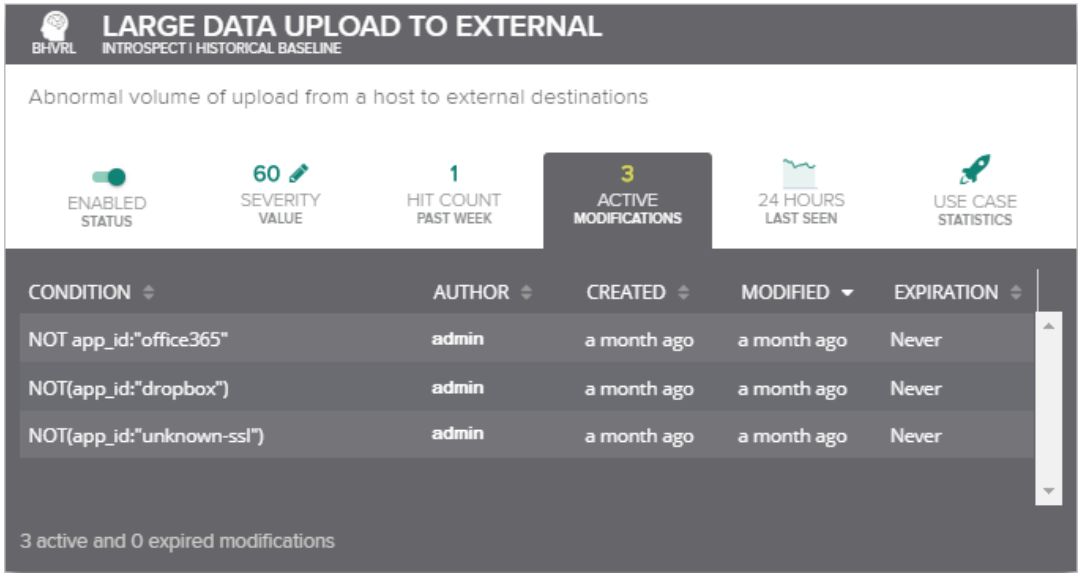


Use Case Modifications Tab

Modifications for use cases are conditions that act as filters to narrow down the use case data from the available data sources by excluding or including a subset of entities, behaviors or other parameters.

In the example in Figure 22, one of the three modifications for use case **Large Data Upload to External** excludes uploads to Dropbox from consideration for that use case.

Figure 22 *Modifications Tab*

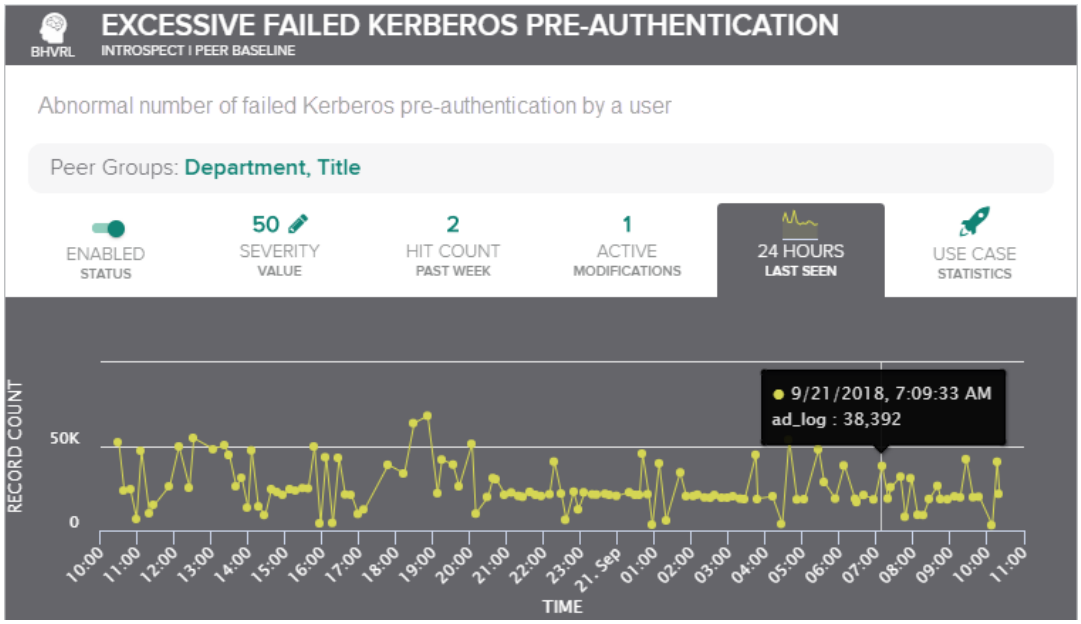


For more information, see Adding Modifications to a Use Case .

Use Case Last Seen Tab

The **Last Seen** tab shows the record count considered for the use case over the last 24 hours. You can mouse-over the points in the graph to view additional log details in a pop-up box.

Figure 23 *Last Seen Tab*



Use Case Statistics Tab

The Statistics tab is a view-only tab. It provides a visual representation of data flowing into the use case over multiple days. This tab displays a heat map where every column corresponds to a single run of the analytics workflow. In general, there is one run per day. The shade of the heat map corresponds to the count of data records in that cell. You can hover on a cell to display a pop-up box with the following information:

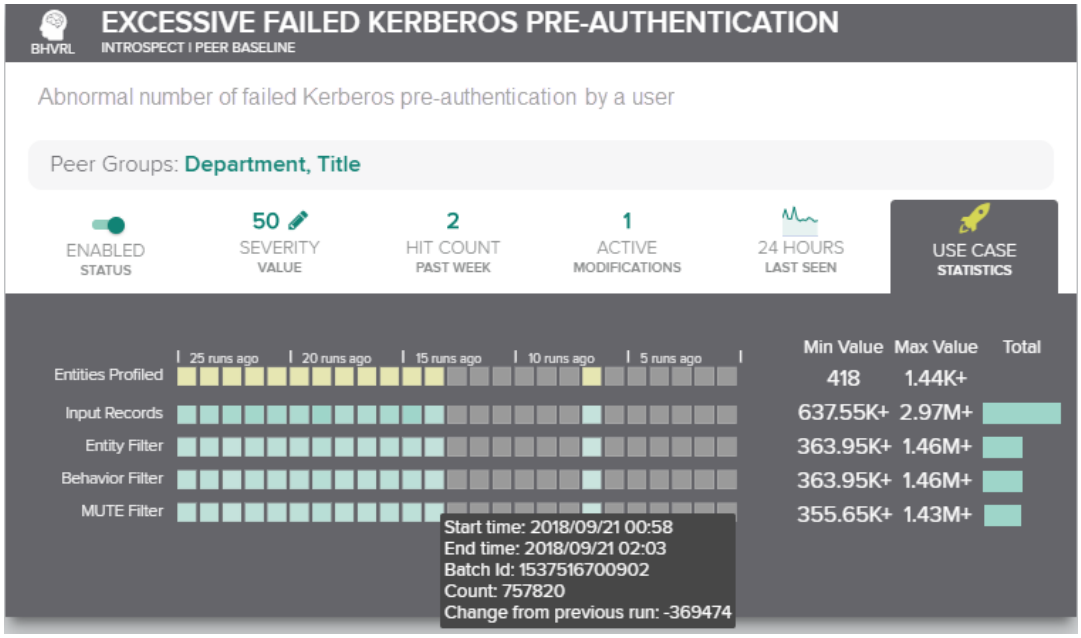
- The start and end time of the run
- The batch ID of the run
- The count which gives you the number of data records
- The change from the previous run

As you follow a single analytics run, going down the column, you can see the data in each row corresponding to the following steps in the sequence:

1. **Entities Profiled**—The number of entities being profiled for that use case across all the entities in the system.
2. **Input Records**—The data records that were input to the use case; this matches the type of data you are trying to send to that use case.
3. **Entity Filter**—The number of entities that pass the entity filter for that use case, which is the subset of entities that you have chosen to profile within that use case.
4. **Behavior Filter**—The data records that match the behavior that you're looking for in the use case.
5. **MUTE Filter**—The data which makes it through the final Modify Use Case To Exclude (MUTE) filter enters the use case.

This visualization enables you to identify issues or problems at a very high level. For example, if you see a stretch of days or runs where there were no entities being profiled, that could indicate that the data flow has been interrupted and must be checked.

Figure 24 *Statistics Tab*



Working with Use Cases

The **Analytics** page displays use cases in a card format. The following tasks can be performed from the **Analytics** page.

- Searching for a Use Case
- Enabling or Disabling Use Cases
- Adding Modifications to a Use Case
- Editing an Existing Use Case
- Cloning a Use Case
- Making Bulk Edits to Use Cases

Searching for a Use Case

To view use cases:

1. Scroll down the **Analytics** page to look for a use case. You can narrow your search as follows:
   a. **Fast Filter**—Type in a word to limit the display of use cases to those matching the use case name, baseline, or description. For example, typing in the word "employee" displays all use cases which contain the word "employee" in either the name, baseline, or description of the use case.
   b. **Filters**—Select options from the categories in the **Filters** pane on the left to limit your search to use cases associated with the selection. The number to the right of each option indicates the number of entries available in the system for that option. Selecting an option in any category automatically updates the remaining **Filters** options to show only those categories that apply to the current selections. The following filter categories are available:
      - **Use Case Type**—Lists two options: **IntroSpect** or pre-defined use cases are provided with the product, and **Custom** use cases are user-defined.
      - **Alert Type**—Available and relevant alert types

- **Use Case Name**—Available and relevant use cases listed by name
- **Baseline**—Entity behavior profile used for comparison to detect abnormalities. Options include: **History**, **Discrete**, **Peer**, and **Chained** baselines.
- **Status**—Enabled or Disabled use cases
- **Data Type**—Data or log sources associated with the use case
- **Attack Stage**—The stage of attack associated with the alerts in the use case

c. **Sort**—Click the **Sort** button at the top of the page to sort the filtered results in  (ascending) or  (descending) order based upon one of the following criteria:

- **Exception Count**
- **False Positive count**
- **Hit Count**
- **Modification Count**
- **Severity**
- **True Positive Count**
- **Use Case Name**

Enabling or Disabling Use Cases

To enable or disable a use case:

1. On the **Analytics** page, locate the use case you need to edit. See Searching for a Use Case for more information on narrowing your search.
2. Notice that disabled use case cards are grayed out on the page until you mouse over them.
3. Click the **Status** switch to change the status for the selected use case to **Enabled** or **Disabled** as needed.
4. When a use case status changes to **Enabled**, it is no longer grayed out. The enabled use case can now generate alerts for the conditions set in it.

Adding Modifications to a Use Case

To add modifications to an existing use case:

1. On the **Analytics** page, locate the use case you need to edit. See Searching for a Use Case for more information on narrowing your search.
2. Click **Actions > Add Modification**.
3. The **Use Case Editor** card opens.
4. Add an optional comment about the modification.
5. Begin typing to see a list of query options. Pick from the options as you build your query sentence.
6. You can use the NOT syntax to add exclusions. For example, NOT(src_ip:"10.32.4.51") to exclude a certain IP address or NOT(user_name:"jdoe") to exclude a certain user.
7. Select an expiry period for the modification. Options range from **Never** to **10 weeks** in one-week increments.
8. Click **Submit**. The **Modifications** tab on the use case should show an increase in the modification count.

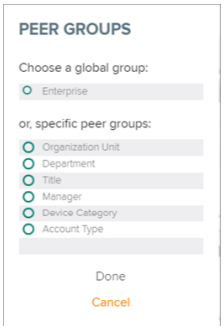
Editing an Existing Use Case

You can modify the configuration of existing use cases by changing the status, severity, and peer groups. You can also add modification queries and specify their duration of activity.

To edit an existing use case:

1. On the **Analytics** page, locate the use case you need to edit. See Searching for a Use Case for more information on narrowing your search.
2. To edit the peer group, you can open the **Peer Groups** pick list by:
   - Clicking the peer group name on the card, or
   - Clicking the **Actions** button next to the use case card. Use **Actions > Select Peer Group(s)**.
3. Select a global or specific peer group and click **Done**. You can select multiple peer groups if desired. In such instances, the use case is run simultaneously for each peer group selected.

Figure 25 *Peer Group Options*



4. To edit the severity, click the pencil icon beside the **Severity** value to edit it inline and enter a new severity level for the alerts you wish to trigger. The severity also factors in to the entity risk score.

Figure 26 *Edit Severity Inline*

5. Click the green checkmark to save the new severity value. A pop-up message indicates that the severity was successfully set. For example: **1use case severity successfully set to 50**.
6. To edit the use case status, click the **Status** switch to enable or disable the use case. Disabled use cases are grayed out on the UI and become highlighted when you mouse over them.
7. You can also select options from the **Actions** button on the right of the card. Depending on the use case, these could include:
   - **View**—Opens a view-only card with details of the use case configuration.
   - **Add Modification**—Opens the Use Case Editor. See Adding Modifications to a Use Case.
   - **Select Peer Group(s)**—Opens the Peer Groups pick list.

Cloning a Use Case

In some instances, you can clone use cases. Cloning allows you to create a copy of a use case and change only a few parameters. For example, you can choose to clone a use case configured to investigate abnormal network access behaviors and change the peer group to detect anomalies specific to that peer group.

NOTE

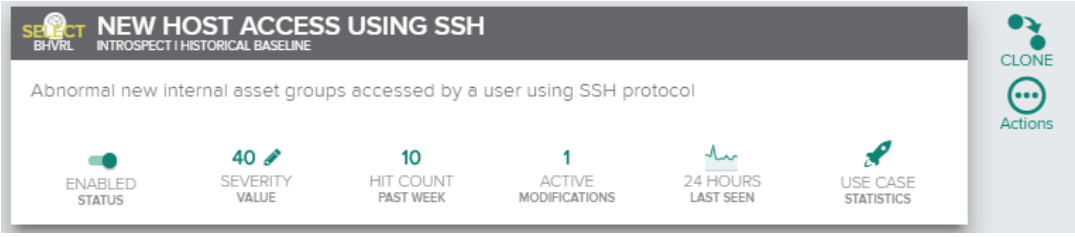
The cloning option is only available for use cases that are behavioral and related to network access activity.

You cannot specify the confidence level for a cloned use case.

To clone a use case:

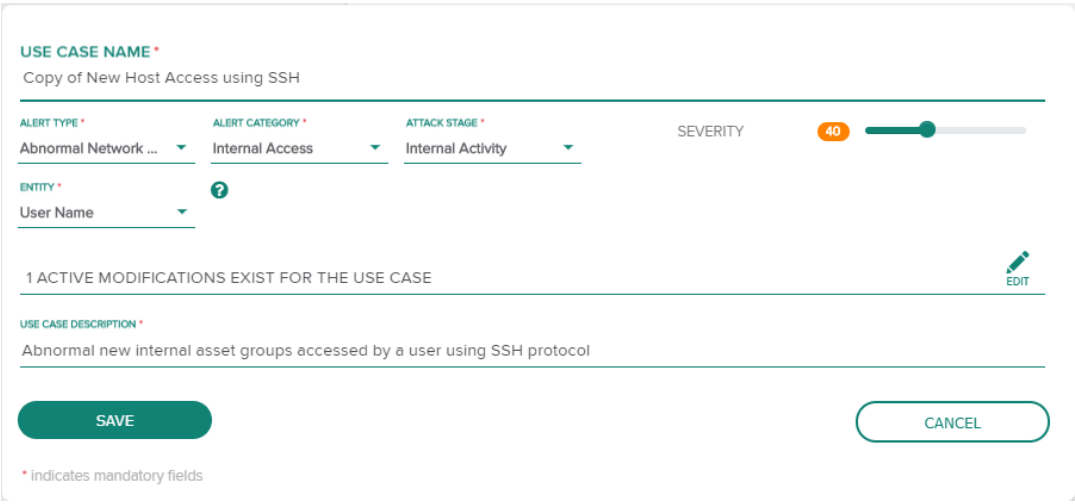
1. On the **Analytics** page, locate the use cases you need to edit. See Searching for a Use Case for more information on narrowing your search.
2. Mouse over the use case card to display the **Clone** option on the right side.

Figure 27 *Use Case Clone Option*



3. Click the **Clone** button. The edit use case card opens showing the use case name with the prefix "Copy of..."

Figure 28 *Editing the Cloned Use Case*



4. Edit the required fields.
5. Click **Save**.

Making Bulk Edits to Use Cases

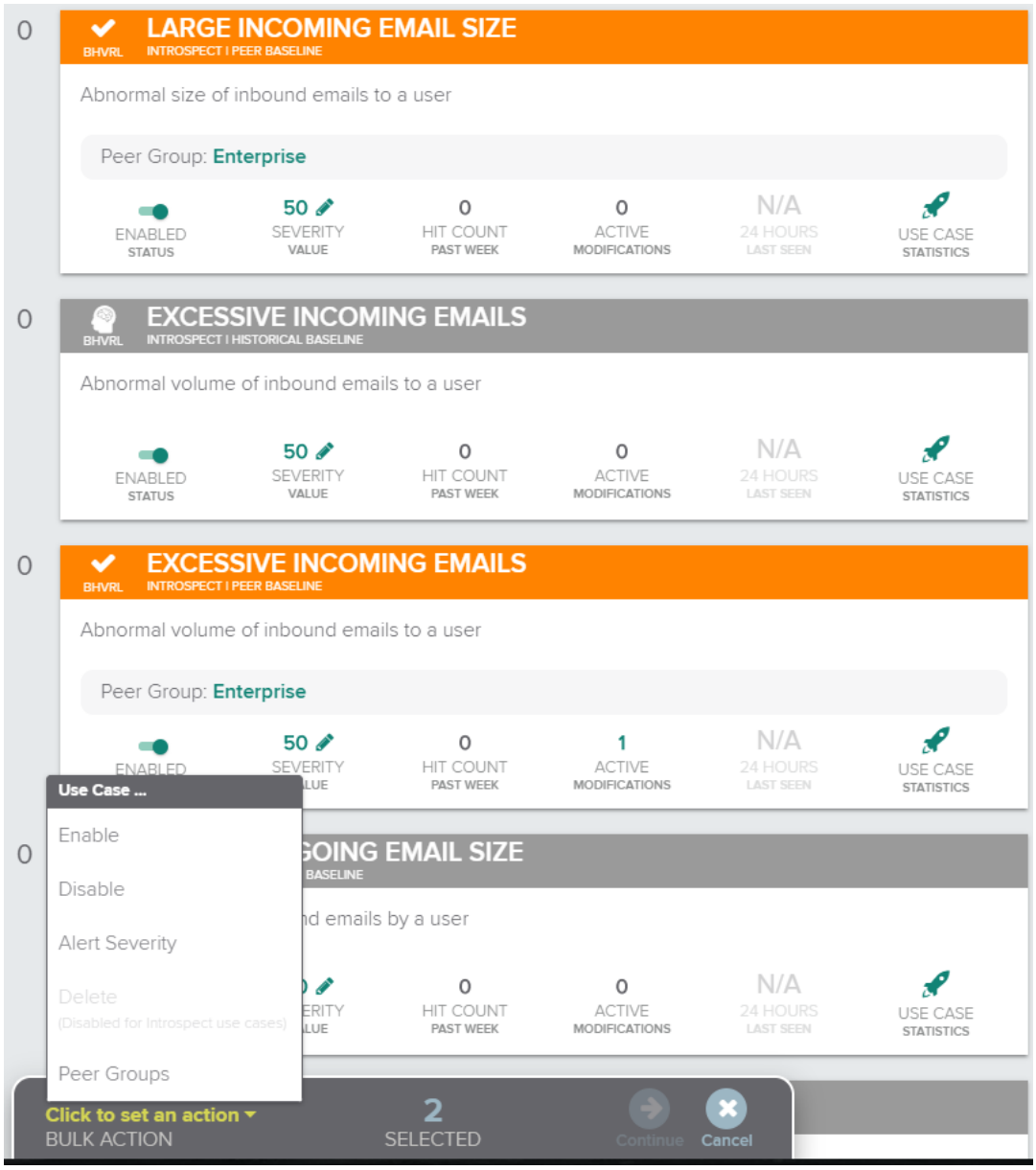
From the Analytics page, you can make edits to a group of use cases. You can individually select multiple use cases to apply a common change or use the **Actions** button at the top of the page to select all use cases which match your filter query, if one was entered.

Option 1: Bulk Edits by Selecting Individual Use Cases

To select use cases individually:

1. On the **Analytics** page, locate the use cases you need to edit. See Searching for a Use Case for more information on narrowing your search.
2. Scroll down the list and click the use case header to select individual use cases. Selected use cases are indicated by a checkmark in the top left corner and the header is highlighted in orange.

Figure 29 *Bulk Edits—Selected Use Cases*



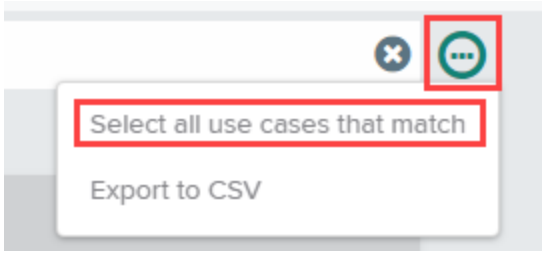
3. In the **Bulk Action** pop-up box which appears at the bottom of the page, click the **Click to set action** link. The **Use Case...** popup box appears with options.
4. Choose the bulk action you wish to apply and click the **Continue** arrow. The next step depends on the options that you have selected:
   - For **Enable**, **Disable**, and **Delete**, the actions are immediately applied and a success message appears with details of the edit such as **1 use case successfully enabled**. IntroSpect use cases cannot be deleted.
   - For **Peer Groups**, the **Peer Groups** pick list appears. Select the peer group and click **Done**.
   - For **Alert Severity**, the **Set Alert Severity** box appears. Use the slider to select a severity level and click **OK**.
5. A success message appears upon completion of the bulk edit.

Option 2: Bulk Edits Using the Actions Button

Another option for bulk edits is available from the **Actions** button at the top of the **Analytics** page.

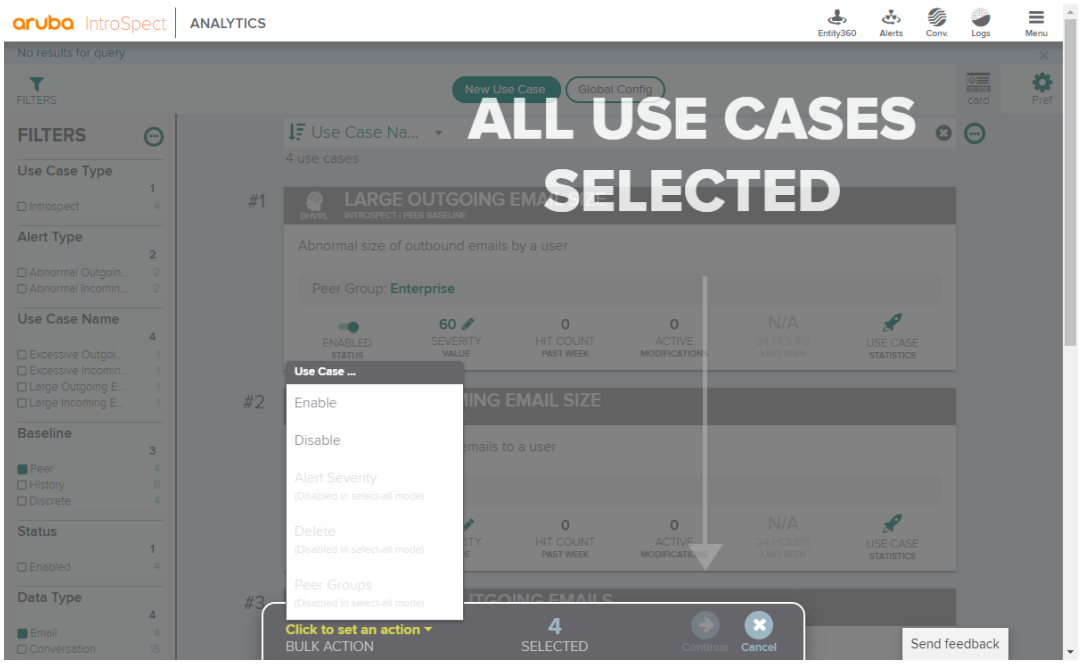
1. On the **Analytics** Page, locate the subset of use cases you need with the help of the facets on the **Filters** pane in conjunction with any filter queries. See Searching for a Use Case for more information on narrowing your search.
2. Click the **Actions** button located at the top of the page, next to the **Search** query field.

Figure 30 *Actions Button on the Analytics Page*



3. Click the **Select all use cases that match** option. An "All Use Cases Selected" message covers the screen and the **Bulk Action** pop-up appears indicating the number of selected use cases.

Figure 31 *Action Button Bulk Edits—All Use Cases Selected*



4. Select an available option and click **Continue** to apply the edit.
5. A success message appears upon completion of the bulk edit.

Creating New Use Cases

Use cases indicate specific contextual behaviors whereas alerts are notifications triggered by conditions defined within that behavioral context or use case.

Adding a New Chained Alert Use Case

Use cases can be behavioral or rule-based. Behavioral use cases are based on the context of an entity's behavior when compared with its own historical data or that of its peers. Alerts are triggered for anomalies detected against this baseline data which can include multiple data records.

To add a new chained alert use case,:

1. On the **Analytics** page, click **New Use Case**.
2. In the options list, select the **Chain > Alert** option.
3. In the new use case card that opens, enter the required information. Mandatory fields are indicated on the card by a red asterisk.

Table 30: *New Use Case—Alert Chain*

Field	Description
Use Case Name	Enter a unique name for the use case, consisting of a brief summary of the use case.
Alert Type	From the dropdown, select the alert type that the use case will trigger.
Alert Category	From the dropdown, select the category to which the alert type belongs.
Attack Stage	From the dropdown, select the stage of attack to which this use case applies.
Min Severity	Use the slider to indicate the level of severity for the alert.
Min Confidence	Use the slider to indicate the level of confidence for the alert.
Time Window	From the dropdown, select the time period within which the sequence of alerts in the chain have to occur.
Associate By	From the dropdown, select the entity with which this use case is associated.
Alert Chain	Use the **Add to Sequence** dropdown to add a sequence of alerts to the chain. The dropdown provides you with various options for quickly locating a specific alert. ■ **Quick Filter**—All alerts available in the system ■ **Alert Categories**—Alerts grouped by Category ■ **Stage**—Alerts grouped by the attack stage of the anomalous behavior or incident ■ **All Alerts**—All alerts available in the system ■ **Add Chain Group**—This option allows you to build a custom group of chained alerts and name it.
Comment	You can add an optional comment to describe the alert sequence.

4. Click **Save.**

Adding a New Rule-Based Use Case

To add a new rule-based use case:

1. On the **Analytics** page, click **New Use Case**.
2. In the options list, select the data type to be considered for the new use case: **AD**, **Conversation**, **Email**, **Third Party Alert**, or **VPN**.
3. In the new rule-based use case card that opens, enter the following information:

Table 31: *New Use Case—Rule-Based*

Field	Description
Use Case Name	Enter a unique name for the use case that provides a brief summary of the use case.
Alert Type	From the dropdown, select the alert type that the use case will trigger.
Alert Category	From the dropdown, select the category to which the alert type belongs.
Attack Stage	From the dropdown, select the stage of attack to which this use case applies.
Severity	Use the slider to indicate the level of severity for the alert.
Confidence	Use the slider to indicate the level of confidence for the alert.
Entity	From the dropdown, select the User, Host, or IP that is associated with the custom use case. The risk score of the entity listed here is updated when the alert is generated.
Query String	Define how the use case is triggered. When the query condition is met, the corresponding alert will be shown. Press the spacebar or begin typing to see a list of options for building the query.
Alert String Template	Enter a sentence with the alert information to be displayed on the alert card when the alert is generated for this use case.
Modifications	(Optional) Add modifications to the use case. These are additional conditions to be met for the alert to trigger.
Use Case Description	(Optional) Enter an additional description to be shown on the use case card. This is a more descriptive summary of the use case and will be displayed under the use case name.

4. Click **Save**.

Custom Use Cases and Resulting Alerts

Use cases are configured to identify specific contextual behaviors and alerts are notifications triggered by conditions defined within that behavioral context. This section provides examples of:

- Custom use cases based on specific data types used in their configuration
- Alerts triggered by each use case

Use Case Based on AD Log Data

Figure 32 shows a custom AD log based use case named: **Disabled Account Logon Custom**.

The resulting alert from this use case is shown in Figure 33.

Figure 32 *Custom AD Use Case*

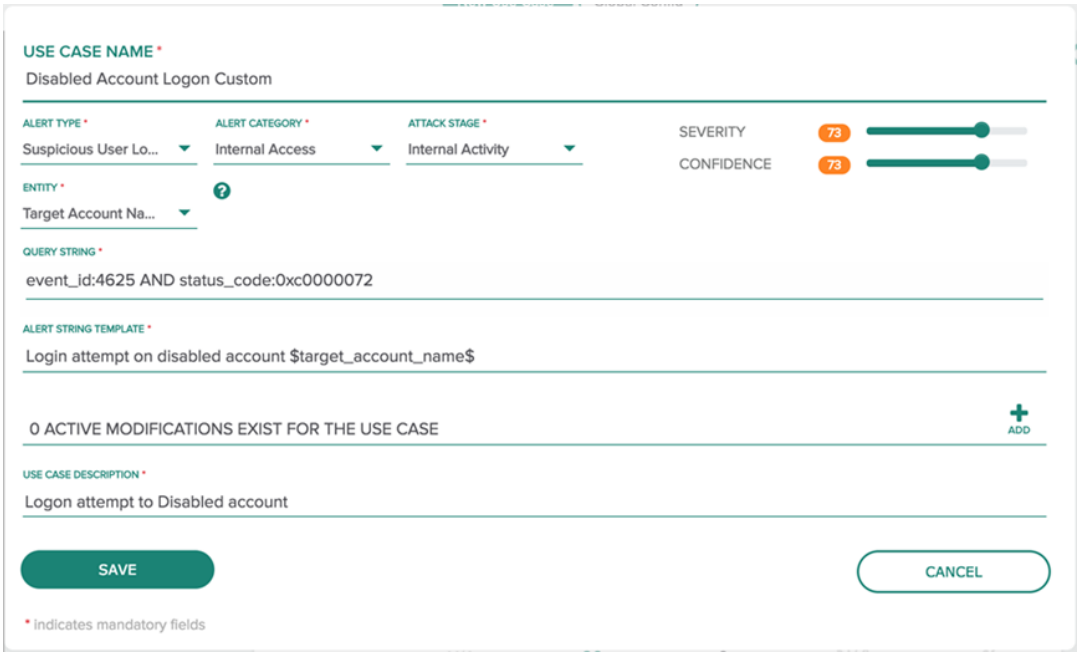
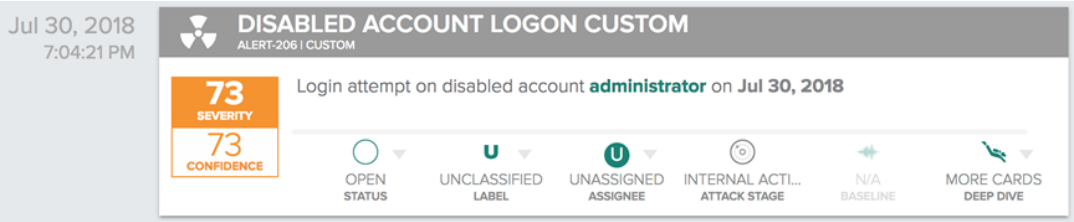


Figure 33 *Alert from Custom AD Use Case*



Use Case Based on Conversations (Eflow) Data

Figure 34 shows a custom eflow based use case named: **HTTP Traffic over non standard port**.

The resulting alert from this use case is shown in Figure 35 .

Figure 34 *Custom Conversations (Eflow) Use Case*

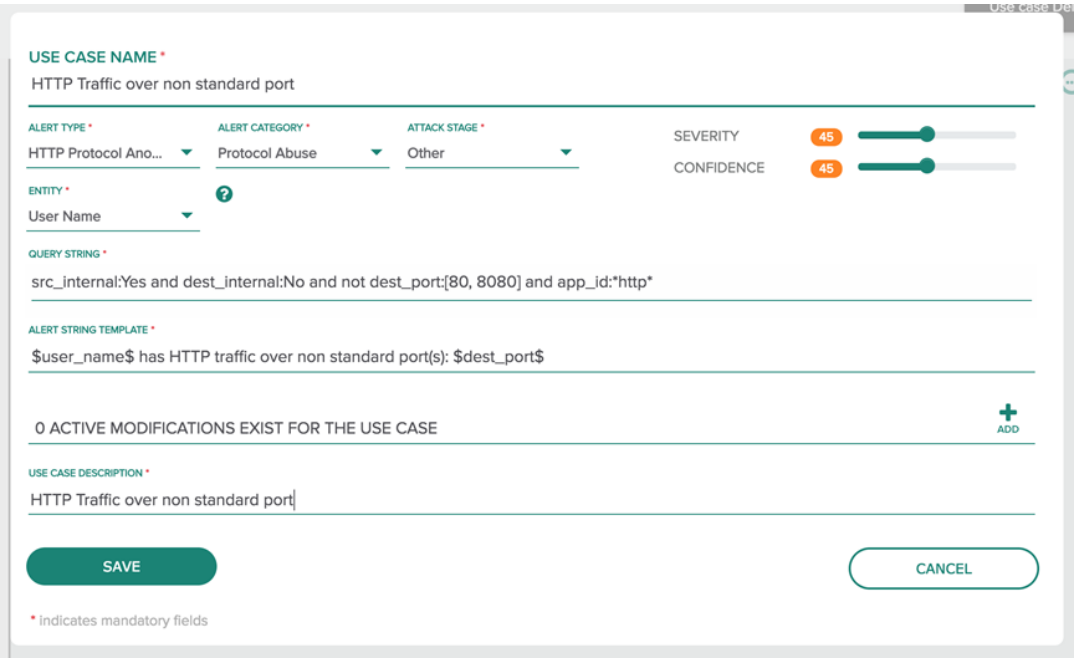
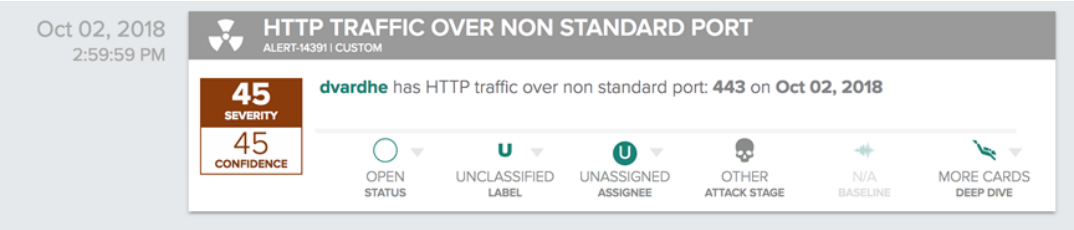


Figure 35 *Alert from Custom Conversations (Eflow) Use Case*



Use Case Based on Email Data

Figure 36 shows a custom email based use case named: **Email from suspicious email address**.

The resulting alert from this use case is shown in Figure 37.

Figure 36 *Custom Email Use Case*

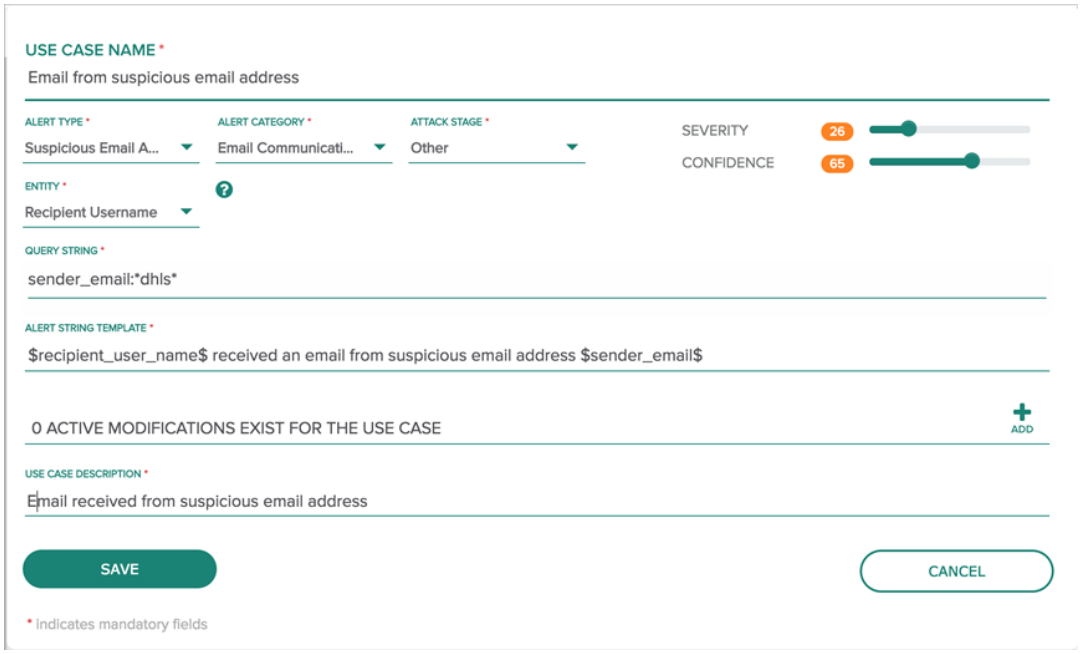
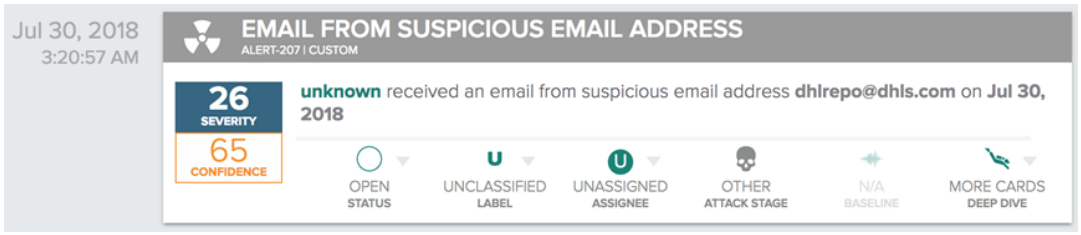


Figure 37 *Alert from Custom Email Use Case*



Use Case Based on Third Party Alerts

Figure 38 shows a custom third-party alert log based use case named: **Splunk Notable custom alert**.

The resulting alert from this use case is shown in Figure 39.

Figure 38 *Custom Third Party Alert Use Case*

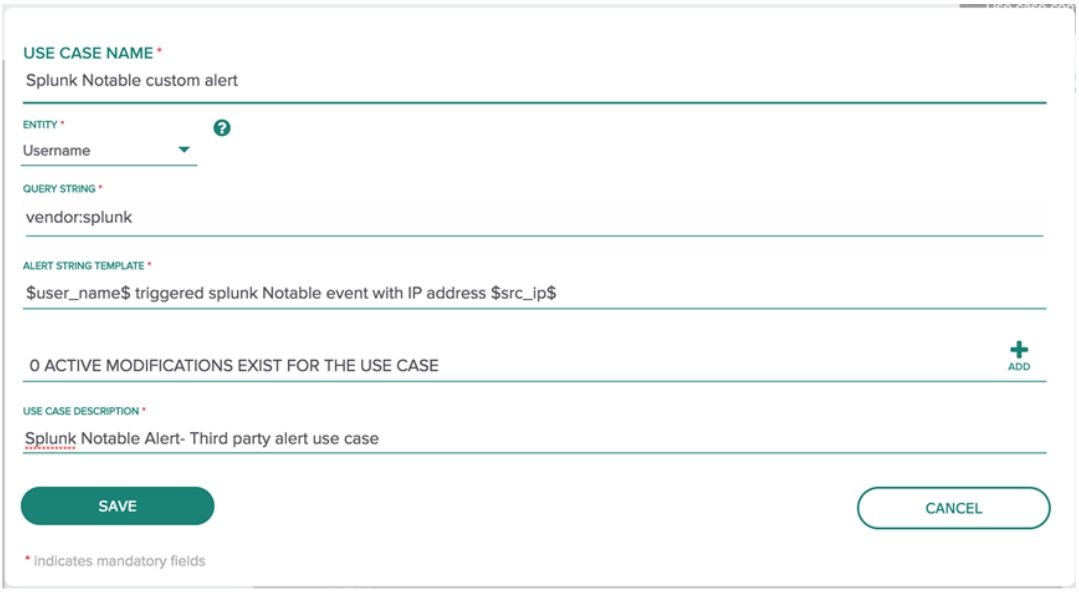


Figure 39 *Alert from Custom Third Party Alert Use Case*

Use Case Based on VPN Logs

Figure 40 shows a custom VPN log based use case named: **Custom VPNLOG Use Case**.

The resulting alert from this use case is shown in Figure 41.

Figure 40 *Custom VPN log Use Case*

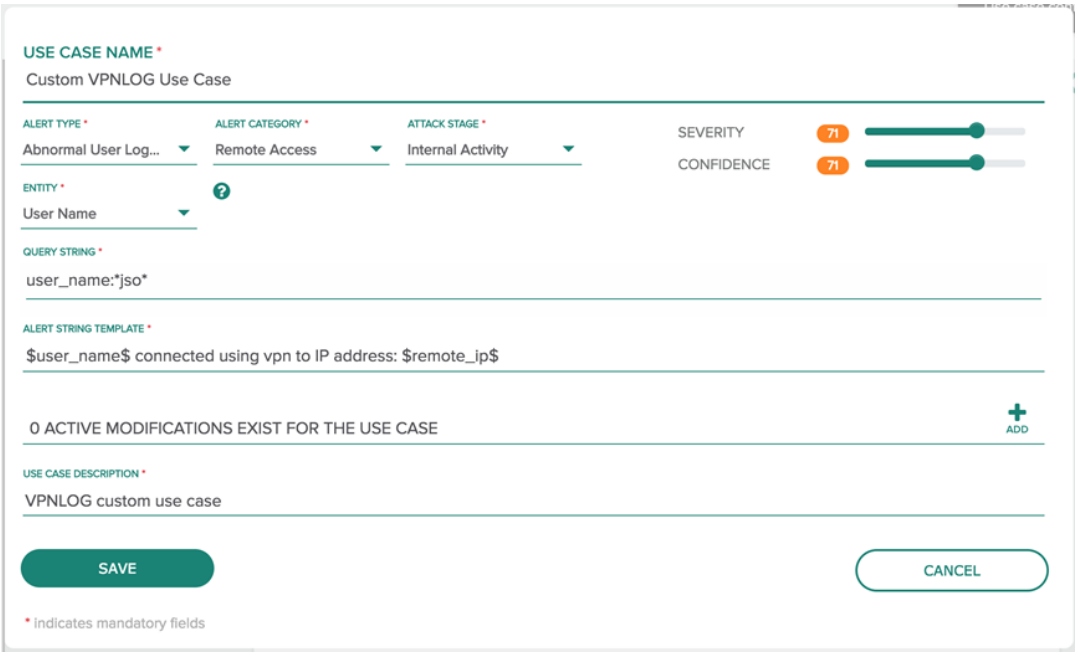


Figure 41 *Alert from Custom VPN Log Use Case*

Global Configuration

The **Global Configuration** tab is available from **Menu > Analytics > Global Config**uration. On this page, you can configure the following global settings that apply across all use cases:

- High Value Asset
- Domain Whitelists
- Trusted Email Domains

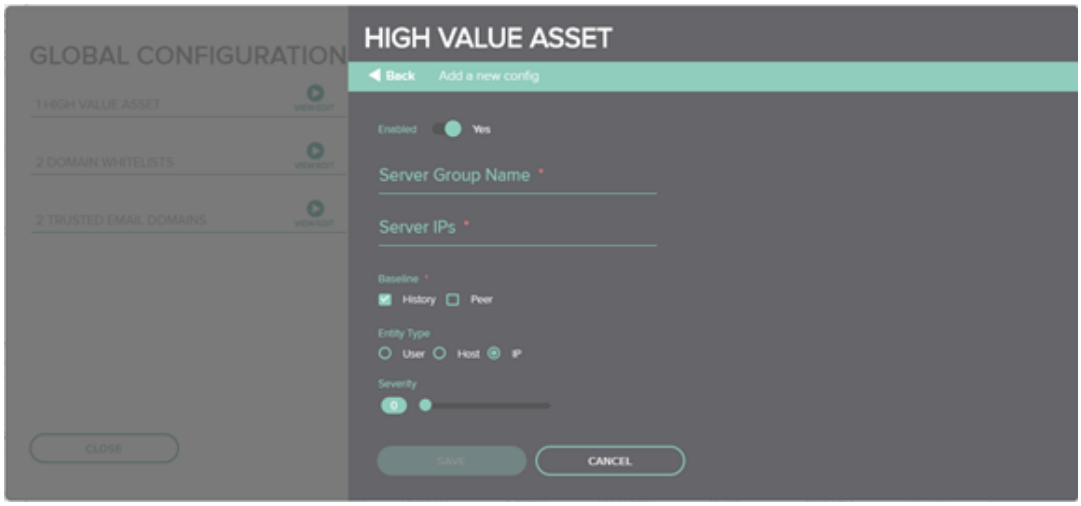
Configuring a High Value Asset

This configuration allows you to create a target list of servers that you want to monitor and profile against.

To configure a **High Value Asset**:

1. Go to **Menu > Analytics > Global Configuration** and select **High Value Asset**. The **High Value Asset** edit window opens.
2. Click **New**. The new **High Value Asset** card opens.

Figure 42 *High Value Asset Card*



3. Configure the following fields and click **Save** when you are done.

Table 32: *High Value Asset Configuration*

Field	Definition
Enabled	Toggle to **Yes** if you wish to enable this configuration after publishing it.
Server Group Name	Enter a name for the server group.
Server IPs	Enter the IP addresses of the servers in the group.
Baseline	Select the baseline data agaisnt which you wish to confgure the profiling.
Entity Type	Select the type of entity you wish to profile.
Severity	Select a severity level for the alerts.

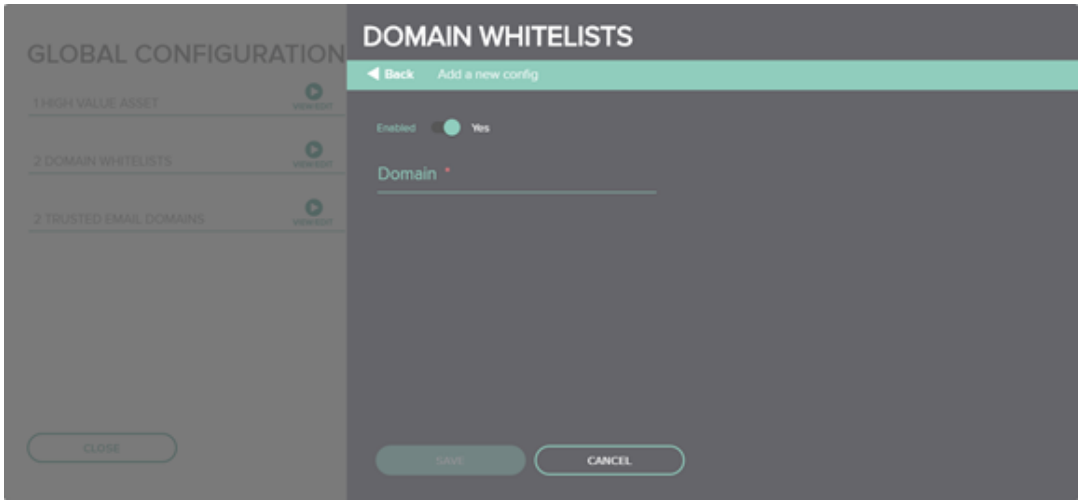
Configuring a Domain Whitelist

This configuration allows you to specify a domain across all use cases, rather than having to go in and specify a domain in an individual query for a new condition.

To configure **Domain Whitelists**:

4. Go to **Menu > Analytics > Global Config**uration and select **Domain Whitelists**. The **Domain Whitelists** edit window opens.
5. Click **New**. The new **Domain Whitelists** card opens.

Figure 43 *Domain Whitelists Card*



6. Configure the following fields and click **Save** when you are done:

Table 33: *Domain Whitelists Configuration*

Field	Definition
Enabled	Toggle to **Yes** if you wish to enable this configuration after publishing it.
Domain	Enter the domain names ypou wish to add to the whitelist.

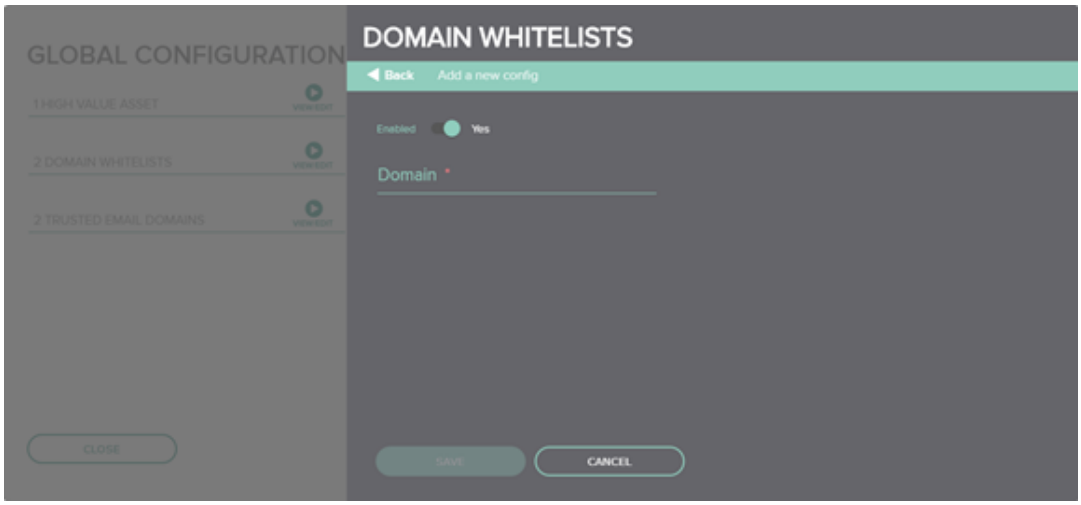
Configuring a New Trusted Email Domain

This configuration allows you to specify email domains that are trusted in your network environment.

To configure **Trusted Email Domains**:

7. Go to **Menu > Analytics > Global Config**uration and select **Trusted Email Domains**. The **Trusted Email Domains** edit window opens.
8. Click **New**. The new **Trusted Email Domains** card opens.

Figure 44 *Trusted Email Domains Card*



9. Configure the following fields and click **Save** when you are done:

Table 34: *Domain Whitelists Configuration*

Field	Definition
Enabled	Toggle to **Yes** if you wish to enable this configuration after publishing it.
Domain	Enter the email domain names you wish to add.