

The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive

Take the Hassel out
of your ISE deployment!

K.I.T.T.

Know ISE Through Training

BRKSEC-2897 - Understanding your ISE deployment with C.L.A.R.K.



The bridge to possible

Understanding your ISE deployment with C.L.A.R.K.

Cisco Log Analysis & Remediation Kiosk

Clark Gambrel – Principal Engineer

@clarkgambrel

BRKSEC-2897



#CiscoLive



The bridge to possible

Understanding your ISE deployment with C.L.A.R.K.

Cisco Log Analysis & Remediation Kiosk

Clark Gambrel – Principal Engineer
@clarkgambrel
BRKSEC-2897

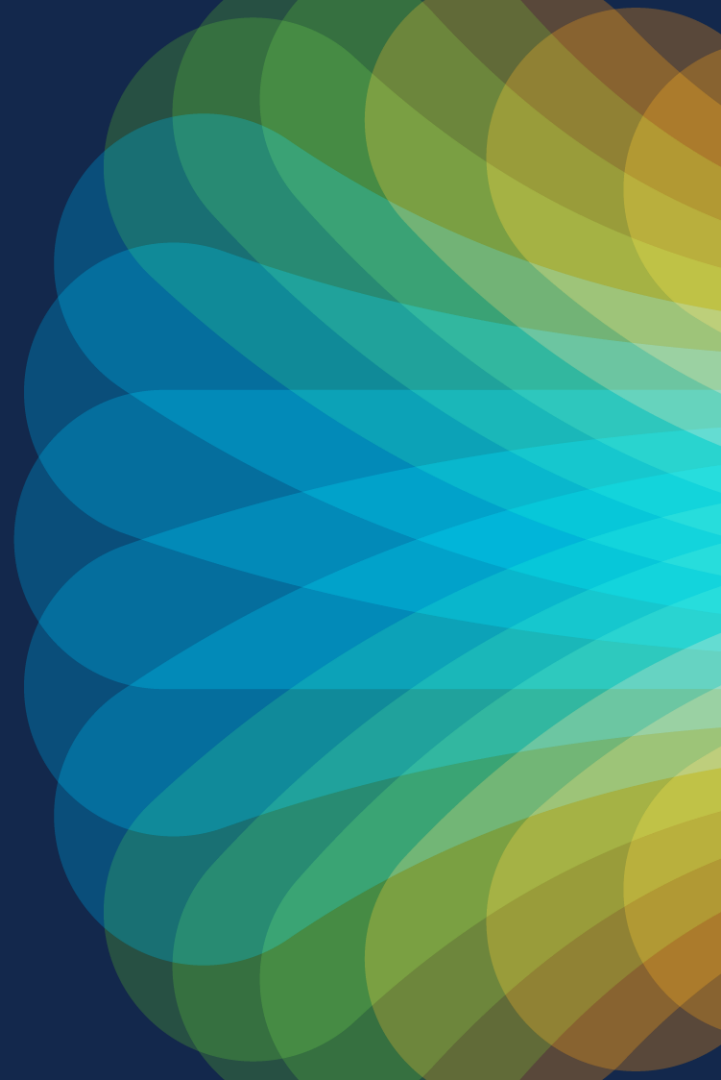
CISCO *Live!*

#CiscoLive

Abstract

The session will help you to understand the health of your ISE deployment and the environment around it. C.L.A.R.K was developed to give deeper visibility into the health and performance of the system and best practices. Now known as "Log Analytics" in ISE 3.2+

Introduction





Clark Gambrel, CCIE #18179

Principal Engineer

cgambrel@cisco.com



@ClarkGambrel





Clark Gambrel, CCIE #18179

Principal Engineer

cgambrel@cisco.com



@ClarkGambrel





KENTUCKY

"I might be a redneck"

How To Find KENTUCKY on the Map



Agenda

- Introduction
- All right stop
Collaborate and listen
(Housekeeping)
- Hay in the needlestack
(manual log analysis)
- The new TPS (MnT reports)
- ISE is back with a brand-new
invention (Log Analytics)
- If there was a problem
Yo, I'll solve it (setup)
- Conclusion

Housekeeping

Cisco Webex App

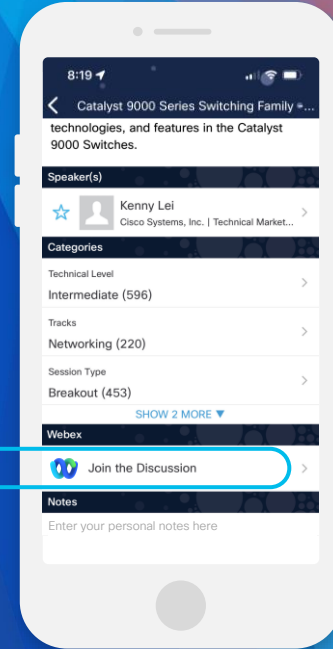
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2897>

Fill out your session surveys!



Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



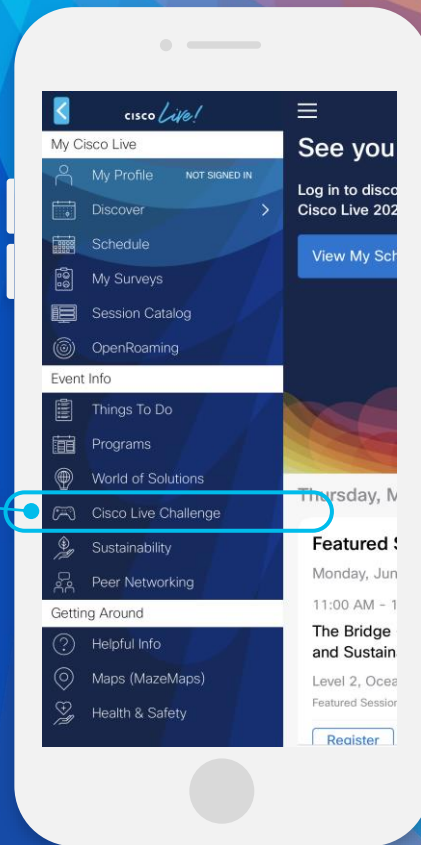
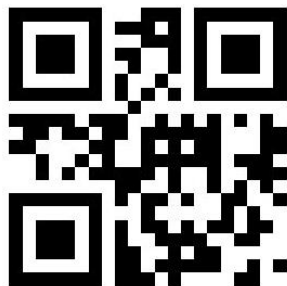
These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Cisco Live Challenge

Gamify your Cisco Live experience!
Get points for attending this session!

How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:



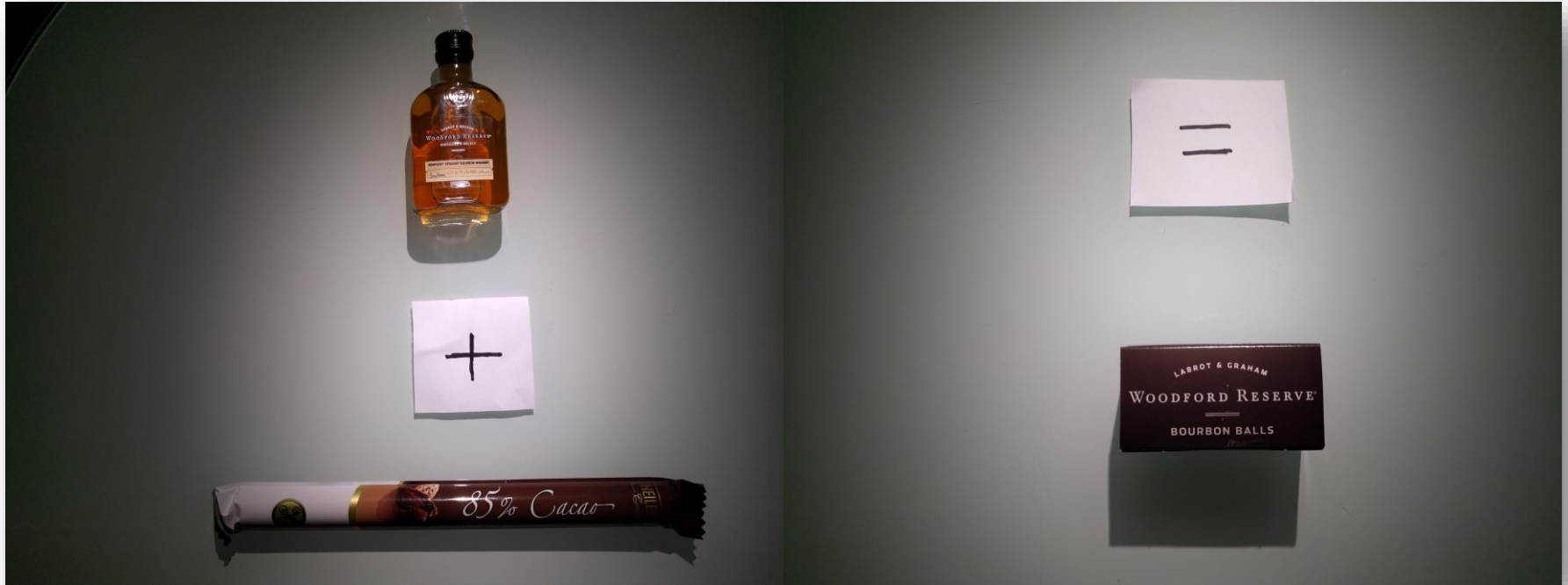
Continue your education

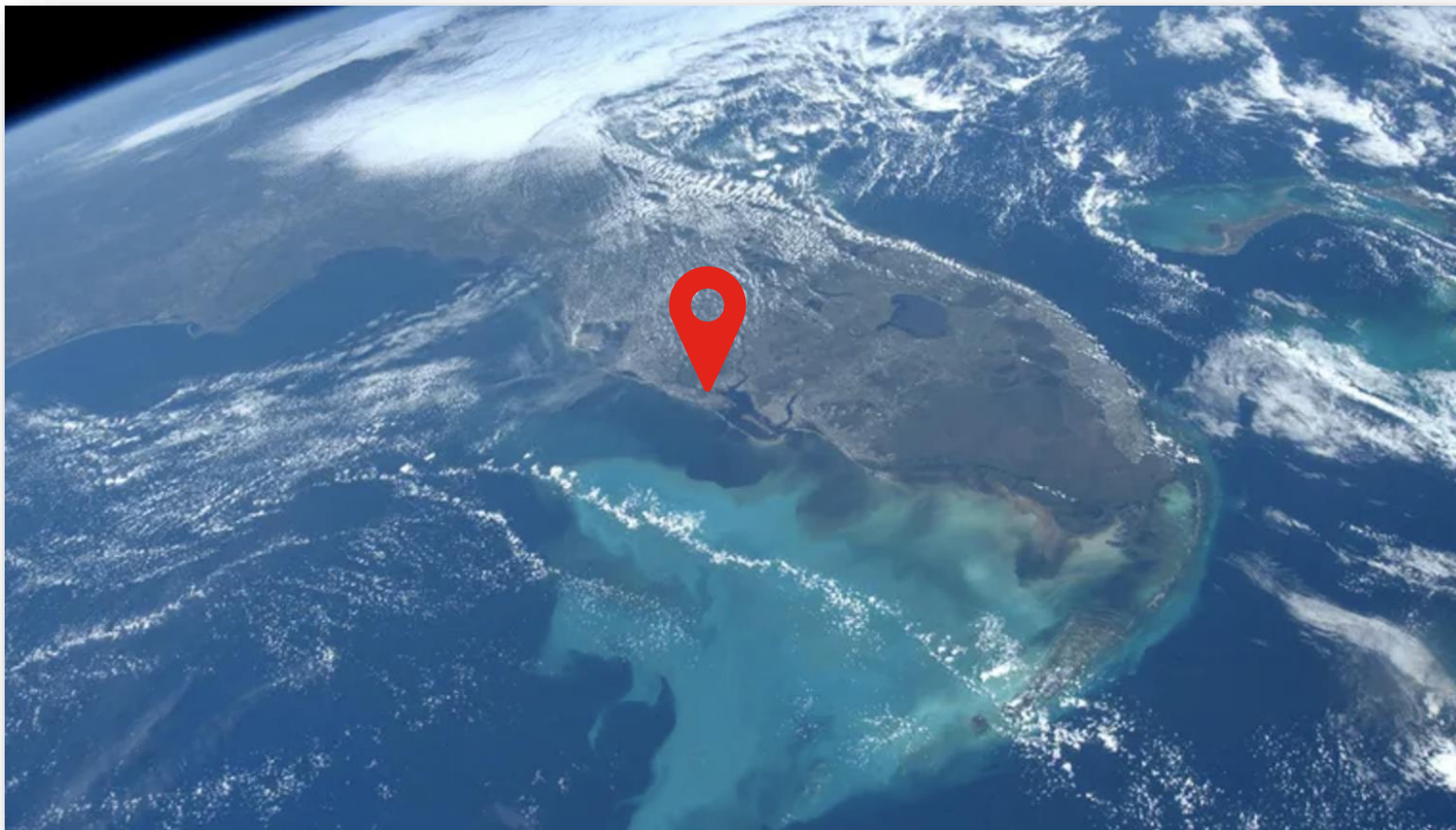


- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Please ask questions!!!

"What are bourbon balls?"







Manual Log Analysis

Manual Log Analysis

Hay in a Needlestack

- Manually searching log files
 - Time consuming
 - No correlation between files
 - Inconsistent formats means custom searches
 - Easy to miss spikes and anomalies
 - No wholistic view
 - Must be done per node
 - Painful use of time



MnT Reports

MnT Reports

The new TPS report

- Default reporting in ISE with MnT
 - Minimal customization
 - No real grouping between dashboards
 - No granularity
 - Easy to miss spikes and anomalies

Log Analytics

Log Analytics

ISE is back with a brand-new invention

- Moving to better visualization
 - Customizable
 - Real grouping between dashboards
 - Granularity
 - Easy to spot spikes and anomalies

Log Analytics

Key Points

- Uses secondary MnT
- Data is derived from the same data that is sent to the MnT node for reporting
- Data is not synchronized between the two MnT nodes
- Configuration changes made in Log Analytics on one MnT will not be updated to the other MnT (Changes must be done on both MnTs. In the future this will be resolved)
- Data is retained for 7 days

Log Analytics

Overview

The screenshot displays the Cisco ISE Operations console interface. At the top, the Cisco ISE logo is on the left, and 'Operations · System 360' is on the right. Below the header, there are three tabs: 'Settings' (which is selected and underlined), 'Monitoring', and 'Log Analytics'. The main content area is titled 'Monitoring and Log Analytics Settings'. It contains two sections. The first section, 'Monitoring', has a blue toggle switch that is turned on. Below it is a link that says 'Go to Monitoring' followed by an external link icon and the word 'View'. The second section, 'Log Analytics', has a grey toggle switch that is turned off, with a black mouse cursor pointing at it. At the bottom right of the settings area, there are two buttons: 'Reset' and 'Save'.

Operations · System 360

Settings Monitoring Log Analytics

Monitoring and Log Analytics Settings

Monitoring enables you to monitor a wide range of applications, system statistics, and key performance indicators (KPI) of all deployment nodes from a centralized console.

☒ Monitoring

Go to [Monitoring](#) View

Log Analytics provides a flexible analytics system for in-depth analysis of syslog data generated from different endpoints.

☐ Log Analytics

Reset Save

Log Analytics

Enabling

Cisco ISE Operations - System 360

Settings Monitoring Log Analytics

Monitoring and Log Analytics Settings

Monitoring enables you to monitor a wide range of applications, system statistics, and key performance indicators (KPI) of all deployment nodes from a centralized console.

☒ Monitoring

Go to [Monitoring](#) [View](#)

Log Analytics provides a flexible analytics system for in-depth analysis of syslog data generated from different endpoints.

☒ Log Analytics

Go to [Log Analytics](#) [View](#)

[Reset](#) [Save](#)

Log Analytics

Dashboards

The screenshot displays the Cisco ISE Log Analytics interface. At the top, the navigation bar includes the Cisco ISE logo and the text 'Operations - System 360'. Below this, a sub-navigation bar shows 'Settings', 'Monitoring', and 'Log Analytics'. The main content area has a dark header with the 'elastic' logo and a search bar labeled 'Search Elastic'. A 'Dashboard' button is highlighted with a mouse cursor. The 'Dashboards' section features a 'Create dashboard' button and a table of existing dashboards.

<input type="checkbox"/>	Title	Description	Tags	Actions
<input type="checkbox"/>	ISE License Dashboard			
<input type="checkbox"/>	ISE Observability Dashboard			
<input type="checkbox"/>	ISE Overview Dashboard			
<input type="checkbox"/>	ISE Processes Summary			
<input type="checkbox"/>	ISE Troubleshooting Dashboard			
<input type="checkbox"/>	Profiler Performance			
<input type="checkbox"/>	Profiler Summary			

Log Analytics

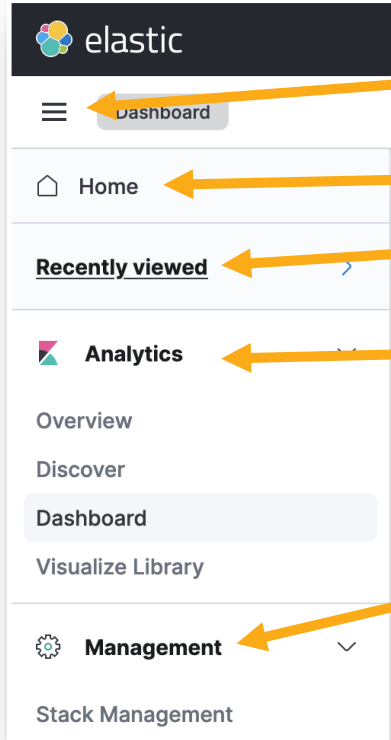
Navigation

The screenshot displays the Cisco ISE Log Analytics interface. At the top, the navigation bar includes the Cisco ISE logo, the text "Operations - System 360", and several utility icons. Below this, a secondary navigation bar shows "Settings", "Monitoring", and "Log Analytics" (which is underlined). The main content area features an "elastic" header with a search bar and a "Dashboard" tab. On the left, a sidebar menu is highlighted with an orange box, containing sections for "Home", "Recently viewed" (listing various dashboards), "Analytics" (with sub-items like Overview, Discover, and Dashboard), and "Management" (with Stack Management). The main area is titled "Dashboards" and includes a "Create dashboard" button. Below this is a search bar and a table of available dashboards.

<input type="checkbox"/>	Title	Description	Tags	Actions
<input type="checkbox"/>	ISE License Dashboard			
<input type="checkbox"/>	ISE Observability Dashboard			
<input type="checkbox"/>	ISE Overview Dashboard			
<input type="checkbox"/>	ISE Processes Summary			
<input type="checkbox"/>	ISE Troubleshooting Dashboard			
<input type="checkbox"/>	Profiler Performance			
<input type="checkbox"/>	Profiler Summary			
<input type="checkbox"/>	RADIUS Accounting Summary			
<input type="checkbox"/>	RADIUS Authentication Summary			

Log Analytics

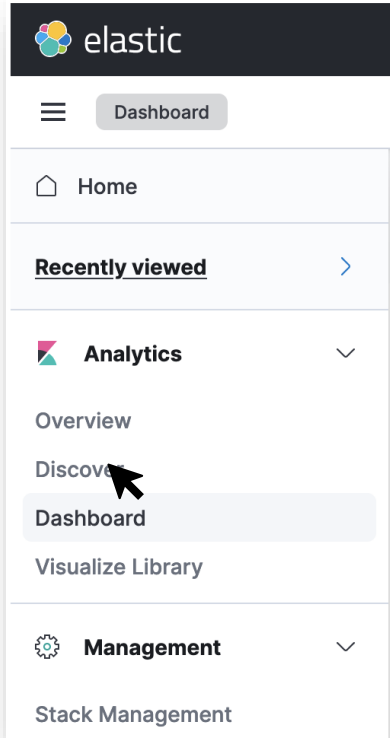
Navigation – Menus



- Menu access
- Homepage for Kibana
- Recent dashboards or visualizations viewed
- Configuration area for visualizations and dashboards
- System settings/configuration

Log Analytics

Navigation – Menus



Log Analytics

Menu - Discover

The screenshot displays the Cisco ISE Log Analytics interface. The top navigation bar includes 'Settings', 'Monitoring', and 'Log Analytics'. The main header shows the 'elastic' logo and a search bar. The 'Discover' tab is active, showing a search bar with 'mnt_analytics_radius*' and a filter by type dropdown. A list of available fields is on the left, including '_id', '_index', '_score', '_type', 'acct_authentic', 'acct_delay_time', 'acct_session_id', and 'acct_session_time'. The main area features a bar chart showing hit counts over time, with a time range of 'May 10, 2023 @ 10:02:29.380 - May 10, 2023 @ 10:17:29.380'. Below the chart, a table of records is displayed, showing timestamps and status types. Annotations with orange arrows point to various UI elements: 'Index Selection' points to the search bar, 'Hit Count' points to the bar chart, 'Time Range' points to the time range selector, 'Filter/Search' points to the filter by type dropdown, 'Records' points to the table of records, and 'Available Fields' points to the list of available fields.

Index Selection

Hit Count

Time Range

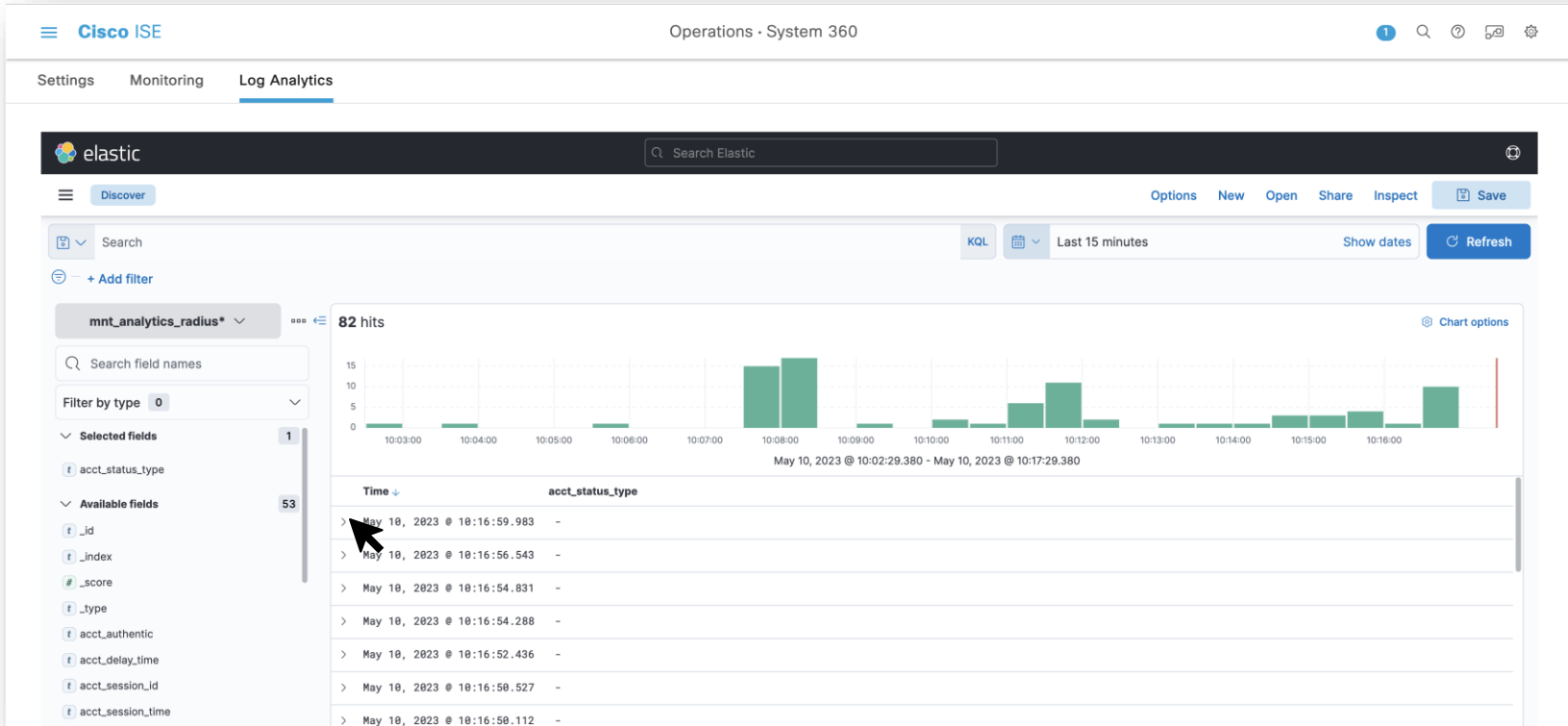
Filter/Search

Records

Available Fields

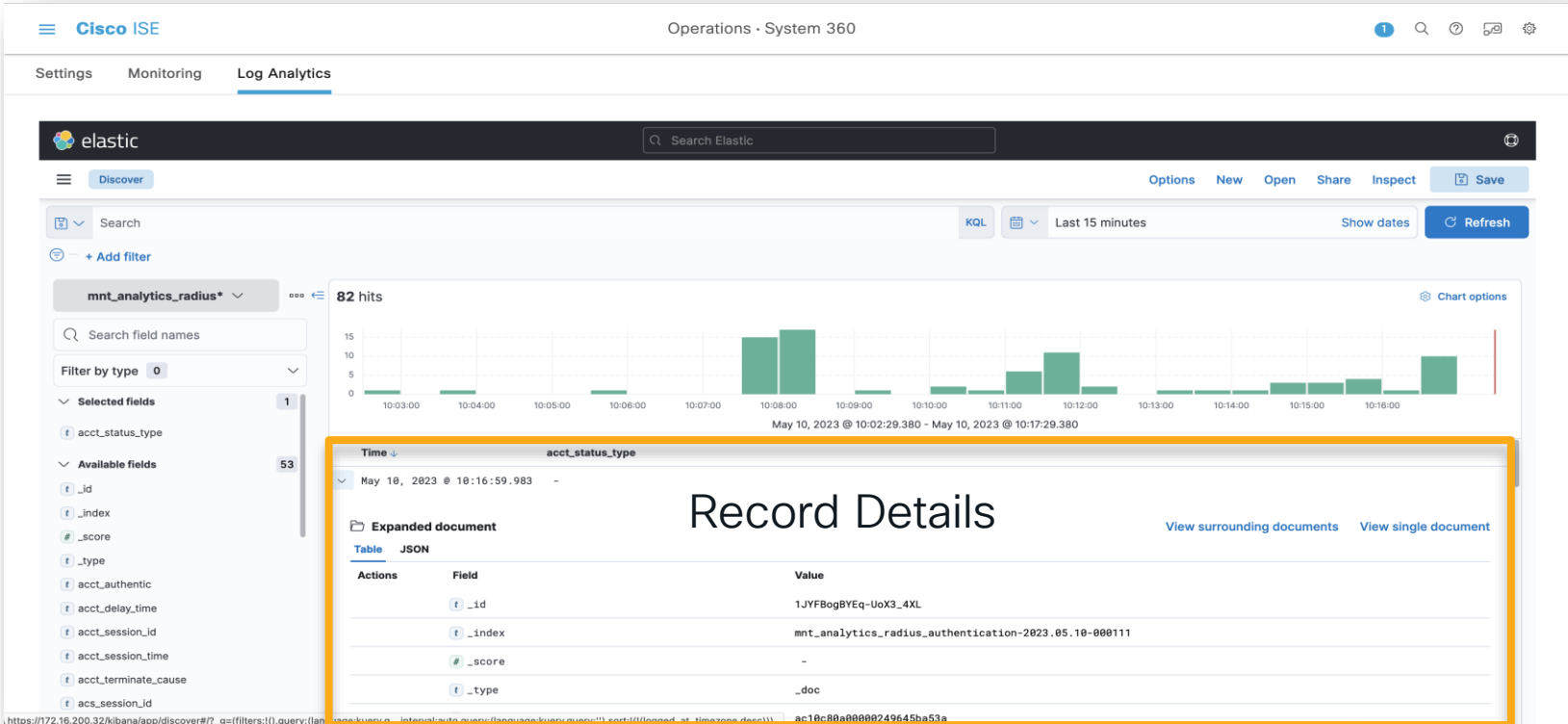
Log Analytics

Menu - Discover



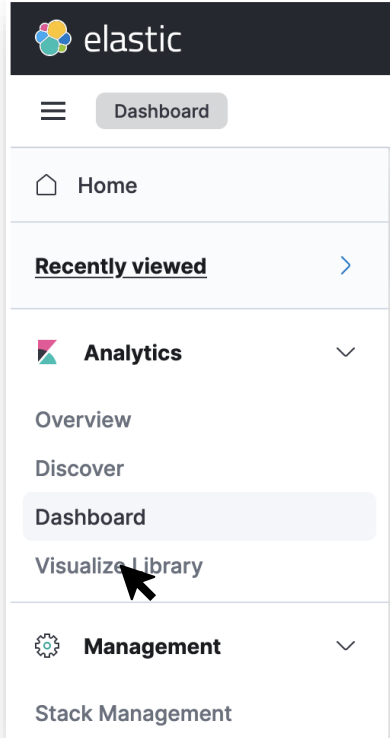
Log Analytics

Menu - Discover



Log Analytics

Navigation – Menus



Log Analytics

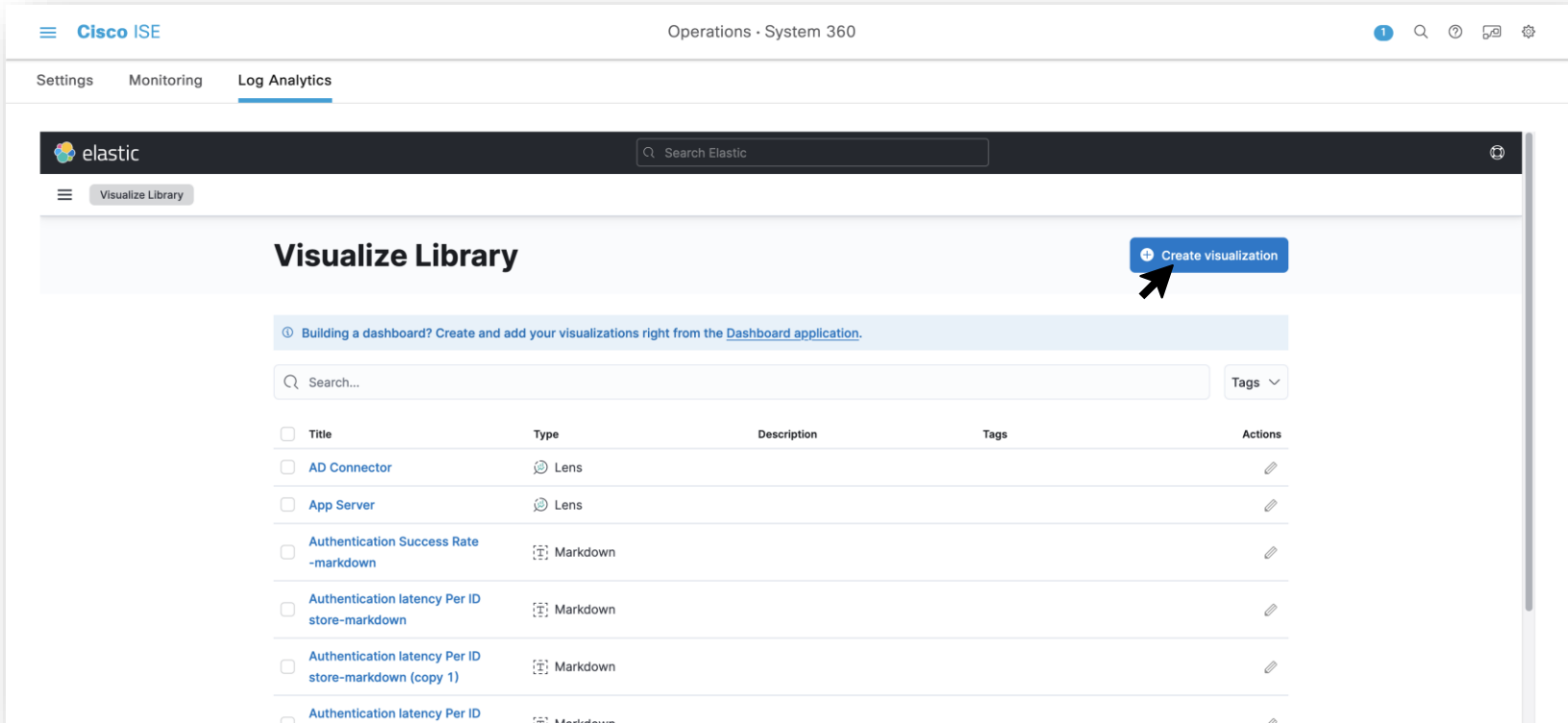
Menu - Visualizations

The screenshot displays the Cisco ISE Log Analytics interface. At the top, the navigation bar includes 'Settings', 'Monitoring', and 'Log Analytics'. Below this, the 'Visualize Library' section is visible, featuring a search bar and a 'Visualize Library' button. The main content area is titled 'Visualize Library' and 'Create'. A blue button labeled 'Create visualization' is highlighted with an orange arrow. Below this, a table lists various visualizations. The 'Authentication Success Rate' row is highlighted with an orange arrow pointing to it from the word 'Select'.

Title	Type	Description	Tags	Actions
<input type="checkbox"/> AD Connector	Lens			
<input type="checkbox"/> App Server	Lens			
<input type="checkbox"/> Authentication Success Rate	Markdown			
<input type="checkbox"/> Authentication latency Per ID store-markdown	Markdown			
<input type="checkbox"/> Authentication latency Per ID store-markdown (copy 1)	Markdown			
<input type="checkbox"/> Authentication latency Per ID	Markdown			

Log Analytics

Visualizations - Create



The screenshot displays the Cisco ISE Log Analytics interface. At the top, the navigation bar includes 'Settings', 'Monitoring', and 'Log Analytics'. The main content area is titled 'Visualize Library' and features a 'Create visualization' button, which is pointed to by a black arrow. Below this button is a search bar and a table of existing visualizations.

Title	Type	Description	Tags	Actions
AD Connector	Lens			
App Server	Lens			
Authentication Success Rate -markdown	Markdown			
Authentication latency Per ID store-markdown	Markdown			
Authentication latency Per ID store-markdown (copy 1)	Markdown			
Authentication latency Per ID	Markdown			

Log Analytics

Visualizations - Create

The screenshot displays the Cisco ISE Log Analytics interface. At the top, the navigation bar includes 'Settings', 'Monitoring', and 'Log Analytics' (which is selected). The main content area shows the 'elastic' search bar and a 'Visualize Library' section. A 'New visualization' modal is open in the center, offering four options: 'Lens' (recommended for most users), 'TSVB' (for time series data), 'Custom visualization' (using Vega syntax), and 'Aggregation based' (using classic charts). The modal also includes a 'Tools' section for adding text, controls, and images. A 'Read documentation' link is provided at the bottom of the modal.

New visualization

- Lens**
Create visualizations with our drag and drop editor. Switch between visualization types at any time. *Recommended for most users.*
- TSVB**
Perform advanced analysis of your time series data.
- Custom visualization**
Use Vega to create new types of visualizations. *Requires knowledge of Vega syntax.*
- Aggregation based**
Use our classic visualize library to create charts based on aggregations.
[Explore options →](#)

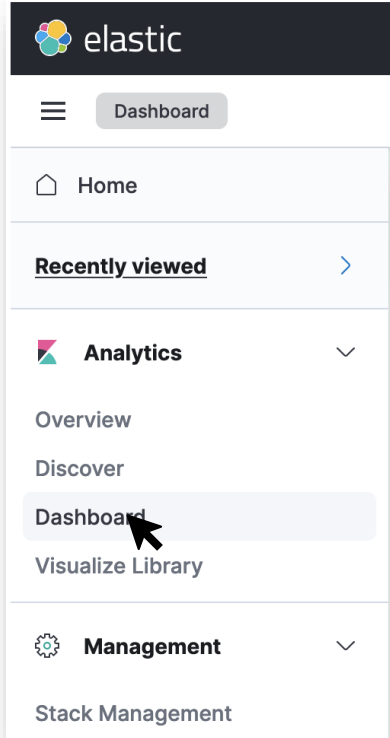
Tools

- Text**
Add text and images to your dashboard.
- Controls**
Add dropdown menus and range sliders to your dashboard.

Want to learn more? [Read documentation](#)

Log Analytics

Navigation – Menus



Log Analytics

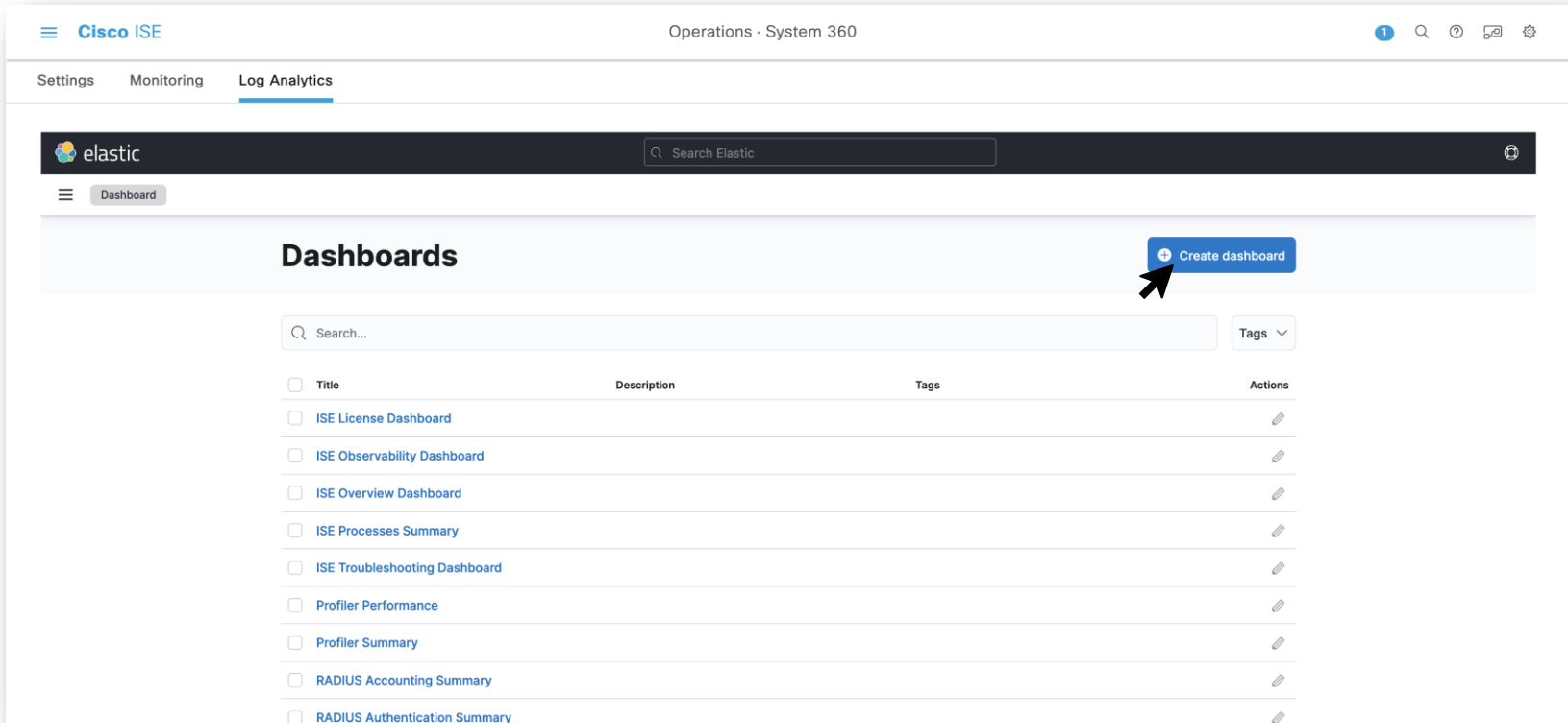
Menu - Dashboards

The screenshot shows the Cisco ISE Log Analytics interface. At the top, there's a navigation bar with 'Cisco ISE' and 'Operations - System 360'. Below that, a breadcrumb trail shows 'Settings', 'Monitoring', and 'Log Analytics'. The main header area has the 'elastic' logo and a search bar. The 'Dashboards' section is active, showing a 'Create' button and a 'Create dashboard' button. Below this is a search bar and a table of dashboards.

Title	Description	Tags	Actions
<input type="checkbox"/> ISE License Dashboard			
<input type="checkbox"/> ISE Observability Dashboard			
<input type="checkbox"/> ISE Overview Dashboard			
<input type="checkbox"/> ISE Processes Summary			
<input type="checkbox"/> ISE Troubleshooting Dashboard			
<input type="checkbox"/> Profiler Performance			
<input type="checkbox"/> Profiler Summary			
<input type="checkbox"/> RADIUS Accounting Summary			
<input type="checkbox"/> RADIUS Authentication Summary			

Log Analytics

Dashboards - Create



The screenshot displays the Cisco ISE Log Analytics interface. At the top, the navigation bar includes 'Settings', 'Monitoring', and 'Log Analytics'. Below this, the 'elastic' logo and a search bar are visible. The main section is titled 'Dashboards' and features a 'Create dashboard' button with a plus icon. A black arrow points to this button. Below the button is a search bar and a 'Tags' dropdown. A table lists existing dashboards with columns for Title, Description, Tags, and Actions.

Title	Description	Tags	Actions
<input type="checkbox"/> ISE License Dashboard			
<input type="checkbox"/> ISE Observability Dashboard			
<input type="checkbox"/> ISE Overview Dashboard			
<input type="checkbox"/> ISE Processes Summary			
<input type="checkbox"/> ISE Troubleshooting Dashboard			
<input type="checkbox"/> Profiler Performance			
<input type="checkbox"/> Profiler Summary			
<input type="checkbox"/> RADIUS Accounting Summary			
<input type="checkbox"/> RADIUS Authentication Summary			

Log Analytics

Dashboards - Create

The screenshot shows the Cisco ISE Log Analytics interface. At the top, there's a navigation bar with 'Cisco ISE' and 'Operations · System 360'. Below it, a sub-navigation bar includes 'Settings', 'Monitoring', and 'Log Analytics'. The main content area has a dark header with the 'elastic' logo and a search bar. Below this, there's a toolbar with 'Dashboard', 'Editing New Dashboard', 'Options', 'Share', 'Switch to view mode', and 'Save'. A search bar with a dropdown arrow is on the left, and 'KQL', a date selector set to 'Last 15 minutes', 'Show dates', and 'Refresh' buttons are on the right. The main area contains two buttons: 'Create visualization' and 'Add from library'. An orange arrow points from the text 'Add Visualizations from Library' to the 'Add from library' button. Another orange arrow points from the text 'Create New Visualization (shortcut)' to the 'Create visualization' button. Below these buttons is a large dashed box with a chart icon and the text 'Add your first visualization' and 'Create content that tells a story about your data.'

Cisco ISE Operations · System 360

Settings Monitoring **Log Analytics**

elastic Search Elastic

Dashboard Editing New Dashboard Options Share Switch to view mode Save

Search KQL Last 15 minutes Show dates Refresh

+ Add filter

Create visualization All types Add from library

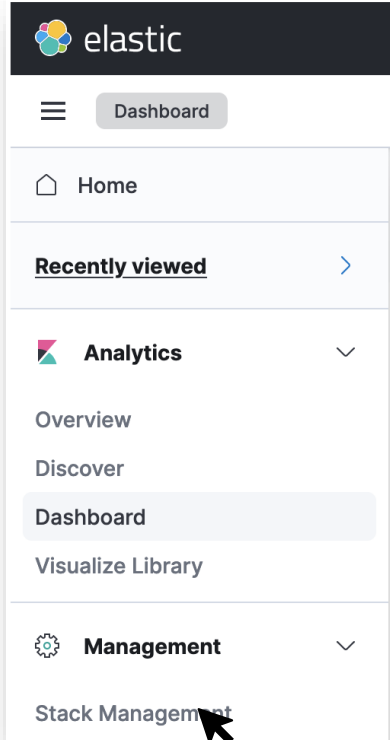
Add your first visualization
Create content that tells a story about your data.

Add Visualizations from Library

Create New Visualization (shortcut)

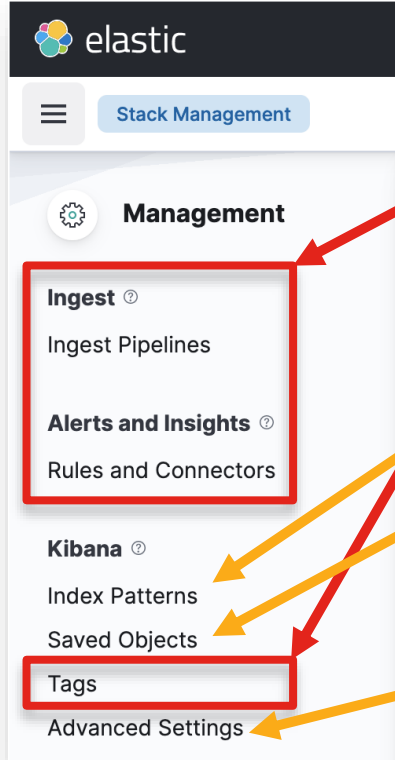
Log Analytics

Navigation – Menus



Log Analytics

Menus – Stack Management



Not currently supported

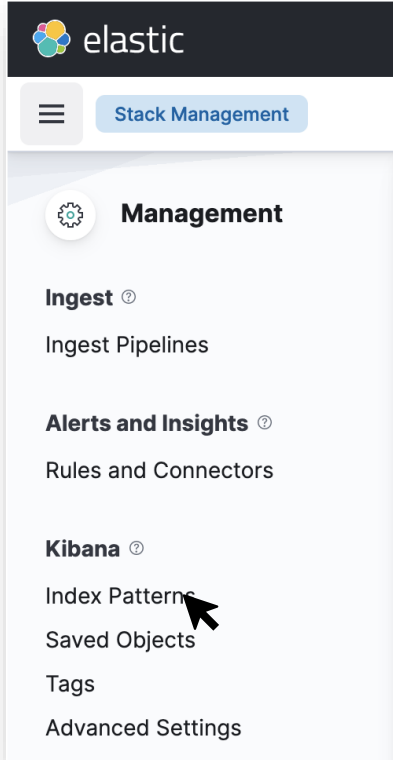
Kibana index search patterns

Import/Export of objects, i.e. dashboards, visualizations, etc.

Kibana settings, i.e. darkmode, timezone, etc.

Log Analytics

Menu - Index Patterns



Log Analytics

Menu - Index Patterns

The screenshot displays the Cisco ISE Log Analytics interface. At the top, the Cisco ISE logo is on the left, and 'Operations - System 360' is on the right. Below the header, there are tabs for 'Settings', 'Monitoring', and 'Log Analytics', with 'Log Analytics' being the active tab. The main content area has a dark header with the 'elastic' logo and a search bar. Below this, there are tabs for 'Stack Management' and 'Index patterns', with 'Index patterns' being the active tab. On the left side of the main content area, there is a 'Management' sidebar with a gear icon. The sidebar contains links for 'Ingest' (with a sub-link 'Ingest Pipelines'), 'Alerts and Insights' (with a sub-link 'Rules and Connectors'), and 'Kibana' (with sub-links 'Index Patterns', 'Saved Objects', 'Tags', and 'Advanced Settings'). The main content area is titled 'Index patterns' and includes a 'Create index pattern' button. Below the title, there is a description: 'Create and manage the index patterns that help you retrieve your data from Elasticsearch.' There is a search bar labeled 'Search...'. Below the search bar, there is a table of index patterns. The table has a header 'Pattern' with an upward arrow. The first row is 'mnt_analytics_tacacs_authentication*' with a 'Default' tag. The other rows are 'mnt_analytics*', 'mnt_analytics_ise_counters*', 'mnt_analytics_license_counters*', 'mnt_analytics_process_status*', 'mnt_analytics_profiler_profiled*', and 'mnt_analytics_radius*'. The interface is clean and modern, with a light blue and white color scheme.

Cisco ISE Operations - System 360

Settings Monitoring Log Analytics

elastic Search Elastic

Stack Management Index patterns

Management

Ingest
Ingest Pipelines

Alerts and Insights
Rules and Connectors

Kibana
Index Patterns
Saved Objects
Tags
Advanced Settings

Index patterns

Create and manage the index patterns that help you retrieve your data from Elasticsearch.

Search...

Pattern ↑

mnt_analytics_tacacs_authentication*	Default
mnt_analytics*	
mnt_analytics_ise_counters*	
mnt_analytics_license_counters*	
mnt_analytics_process_status*	
mnt_analytics_profiler_profiled*	
mnt_analytics_radius*	

Log Analytics

Index Patterns - Create

The screenshot displays the Cisco ISE Log Analytics interface. At the top, the navigation bar includes the Cisco ISE logo, the text 'Operations - System 360', and several utility icons. Below this, a secondary navigation bar shows 'Settings', 'Monitoring', and 'Log Analytics' (which is underlined). The main content area features an 'elastic' header with a search bar. A left sidebar contains a 'Management' section with links to 'Ingest', 'Alerts and Insights', and 'Kibana', with 'Index Patterns' highlighted. The main panel is titled 'Index patterns' and includes a description: 'Create and manage the index patterns that help you retrieve your data from Elasticsearch.' Below this is a search bar and a list of index patterns. The first pattern, 'mnt_analytics_tacacs_authentication*', is marked as 'Default'. Other patterns include 'mnt_analytics*', 'mnt_analytics_ise_counters*', 'mnt_analytics_license_counters*', 'mnt_analytics_process_status*', 'mnt_analytics_profiler_profiled*', and 'mnt_analytics_radius*'. A blue button labeled 'Create index pattern' with a plus icon is located in the top right of the main panel, with a black arrow pointing to it.

Cisco ISE Operations - System 360

Settings Monitoring Log Analytics

elastic Search Elastic

Stack Management Index patterns

Management

- Ingest
- Alerts and Insights
- Kibana
- Index Patterns
- Saved Objects
- Tags
- Advanced Settings

Index patterns

Create and manage the index patterns that help you retrieve your data from Elasticsearch.

Search...

Pattern ↑

- mnt_analytics_tacacs_authentication* **Default**
- mnt_analytics*
- mnt_analytics_ise_counters*
- mnt_analytics_license_counters*
- mnt_analytics_process_status*
- mnt_analytics_profiler_profiled*
- mnt_analytics_radius*

Create index pattern

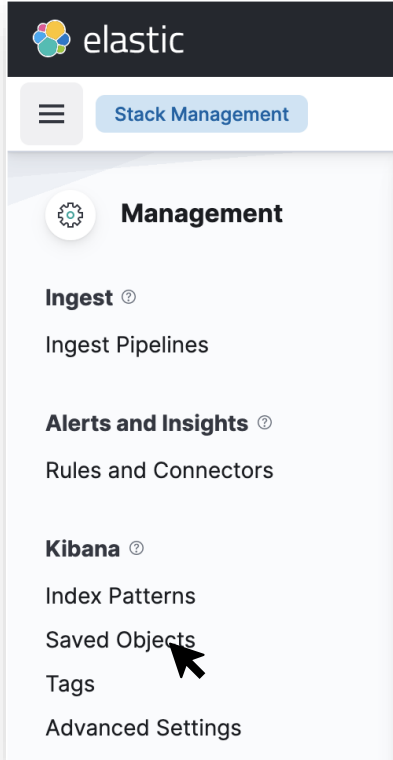
Log Analytics

Index Patterns - Create

[illegible]

Log Analytics

Menu – Saved Objects



Log Analytics

Saved Objects - Menu

The screenshot displays the Cisco ISE Log Analytics interface. At the top, the Cisco ISE logo is on the left, and 'Operations - System 360' is in the center. On the right, there are icons for notifications, search, help, and settings. Below the top bar, a navigation menu shows 'Settings', 'Monitoring', and 'Log Analytics' (which is selected). The main content area has a dark header with the 'elastic' logo and a search bar. Below this, a sub-header shows 'Stack Management' and 'Saved objects' (selected). On the left, a 'Management' sidebar lists 'Ingest' (Ingest Pipelines), 'Alerts and Insights' (Rules and Connectors), and 'Kibana' (Index Patterns, **Saved Objects**, Tags, Advanced Settings). The main panel is titled 'Saved Objects' and includes a description: 'Manage and share your saved objects. To edit the underlying data of an object, go to its associated application.' It features a search bar, 'Refresh', 'Import', and 'Export 202 objects' buttons. Below these are 'Type' and 'Tags' dropdowns, a 'Delete' button, and an 'Export' dropdown. A table lists saved objects with columns for checkboxes, Type, Title, Tags, and Actions. The table contains 10 entries, including 'Advanced Settings [7.17.0]', 'RADIUS Authentication Summary', 'ISE Overview Dashboard', 'ISE Processes Summary', 'TACACS Authentication Summary', 'ISE Observability Dashboard', 'RADIUS Accounting Summary', and 'TACACS Accounting Summary'.

Management

- Ingest ⓘ
Ingest Pipelines
- Alerts and Insights ⓘ
Rules and Connectors
- Kibana ⓘ
Index Patterns
Saved Objects
Tags
Advanced Settings

Saved Objects

Manage and share your saved objects. To edit the underlying data of an object, go to its associated application.

Search Elastic

Stack Management Saved objects

Refresh Import Export 202 objects

Search...

Type Tags Delete Export

<input type="checkbox"/>	Type	Title	Tags	Actions
<input type="checkbox"/>	...	Advanced Settings [7.17.0]		🔍 🔗
<input type="checkbox"/>	📄	RADIUS Authentication Summary		🔍 🔗
<input type="checkbox"/>	📄	ISE Overview Dashboard		🔍 🔗
<input type="checkbox"/>	📄	ISE Processes Summary		🔍 🔗
<input type="checkbox"/>	📄	TACACS Authentication Summary		🔍 🔗
<input type="checkbox"/>	📄	ISE Observability Dashboard		🔍 🔗
<input type="checkbox"/>	📄	RADIUS Accounting Summary		🔍 🔗
<input type="checkbox"/>	📄	TACACS Accounting Summary		🔍 🔗

Log Analytics

Saved Objects - Export

The screenshot shows the Cisco ISE Log Analytics interface. The top navigation bar includes 'Settings', 'Monitoring', and 'Log Analytics'. The 'Log Analytics' section is active, showing a list of 'Saved Objects'. The interface includes a sidebar with 'Management' and 'Kibana' sections. The main area displays a list of saved objects with checkboxes for selection. An orange arrow points from the text 'Select individual objects or export all' to the checkboxes and the 'Export 202 objects' button.

Saved Objects

Manage and share your saved objects. To edit the underlying data of an object, go to its associated application.

Search...

Type Tags Delete Export

Type	Title	Tags	Actions
<input type="checkbox"/>	Advanced Settings [7.17.0]		
<input type="checkbox"/>	RADIUS Authentication Summary		
<input type="checkbox"/>	ISE Overview Dashboard		
<input type="checkbox"/>	ISE Processes Summary		
<input type="checkbox"/>	TACACS Authentication Summary		
<input type="checkbox"/>	ISE Observability Dashboard		
<input type="checkbox"/>	RADIUS Accounting Summary		
<input type="checkbox"/>	TACACS Accounting Summary		

Refresh Import Export 202 objects

Log Analytics

Saved Objects - Export

Cisco ISE Operations - System 360

Settings Monitoring **Log Analytics**

elastic Search Elastic

Stack Management Saved objects

Management

- Ingest[Ⓢ]
Ingest Pipelines
- Alerts and Insights[Ⓢ]
Rules and Connectors
- Kibana[Ⓢ]
Index Patterns
Saved Objects
Tags
Advanced Settings

Saved Objects

Manage and share your saved objects. To edit the underlying data of an object, go to its associated application.

Refresh Import Export 202 objects

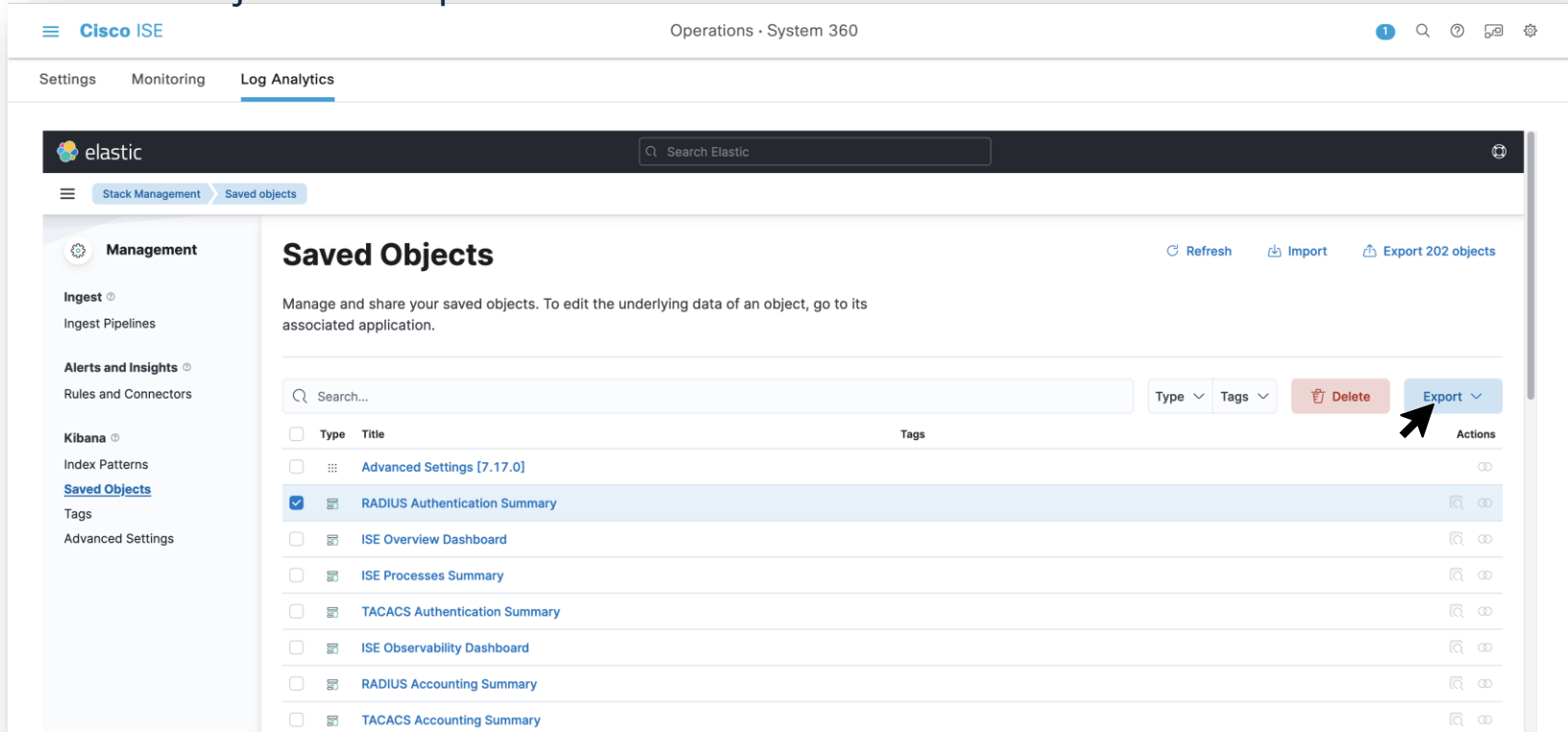
Search...

Type Tags Delete Export

Type	Title	Tags	Actions
<input type="checkbox"/>	Advanced Settings [7.17.0]		
<input checked="" type="checkbox"/>	RADIUS Authentication Summary		
<input type="checkbox"/>	ISE Overview Dashboard		
<input type="checkbox"/>	ISE Processes Summary		
<input type="checkbox"/>	TACACS Authentication Summary		
<input type="checkbox"/>	ISE Observability Dashboard		
<input type="checkbox"/>	RADIUS Accounting Summary		
<input type="checkbox"/>	TACACS Accounting Summary		

Log Analytics

Saved Objects - Export



The screenshot displays the Cisco ISE Log Analytics interface. The top navigation bar shows 'Cisco ISE' and 'Operations - System 360'. The left sidebar contains 'Settings', 'Monitoring', and 'Log Analytics' (selected). The main content area is titled 'Saved Objects' and includes a search bar, 'Refresh', 'Import', and 'Export 202 objects' buttons. A table lists saved objects with columns for 'Type', 'Title', and 'Actions'. The 'RADIUS Authentication Summary' object is selected. An arrow points to the 'Export' button in the 'Actions' column.

Type	Title	Tags	Actions
<input type="checkbox"/>	Advanced Settings [7.17.0]		
<input checked="" type="checkbox"/>	RADIUS Authentication Summary		
<input type="checkbox"/>	ISE Overview Dashboard		
<input type="checkbox"/>	ISE Processes Summary		
<input type="checkbox"/>	TACACS Authentication Summary		
<input type="checkbox"/>	ISE Observability Dashboard		
<input type="checkbox"/>	RADIUS Accounting Summary		
<input type="checkbox"/>	TACACS Accounting Summary		

Log Analytics

Saved Objects - Export

The screenshot shows the Cisco ISE Log Analytics interface. The top navigation bar includes 'Settings', 'Monitoring', and 'Log Analytics'. The main content area is titled 'Saved Objects' and contains a table of saved objects. The 'RADIUS Authentication Summary' object is selected. An 'Export' button is visible, and a tooltip shows options to 'Include related objects' and 'Export'.

Choose to include dependencies

Type	Title	Tags
<input type="checkbox"/>	Advanced Settings [7.17.0]	
<input checked="" type="checkbox"/>	RADIUS Authentication Summary	
<input type="checkbox"/>	ISE Overview Dashboard	
<input type="checkbox"/>	ISE Processes Summary	
<input type="checkbox"/>	TACACS Authentication Summary	
<input type="checkbox"/>	ISE Observability Dashboard	
<input type="checkbox"/>	RADIUS Accounting Summary	
<input type="checkbox"/>	TACACS Accounting Summary	

Log Analytics

Saved Objects - Export

Operations - System 360

Settings Monitoring **Log Analytics**

elastic Search Elastic

Stack Management Saved objects

Management

- Ingest
Ingest Pipelines
- Alerts and Insights
Rules and Connectors
- Kibana
Index Patterns
Saved Objects
Tags
Advanced Settings

Saved Objects

Manage and share your saved objects. To edit the underlying data of an object, go to its associated application.

Refresh Import Export 202 objects

Search...

Type Tags Delete Export

Type	Title	Tags	Actions
<input type="checkbox"/>	Advanced Settings [7.17.0]		
<input checked="" type="checkbox"/>	RADIUS Authentication Summary		
<input type="checkbox"/>	ISE Overview Dashboard		
<input type="checkbox"/>	ISE Processes Summary		
<input type="checkbox"/>	TACACS Authentication Summary		
<input type="checkbox"/>	ISE Observability Dashboard		
<input type="checkbox"/>	RADIUS Accounting Summary		
<input type="checkbox"/>	TACACS Accounting Summary		

Log Analytics

Saved Objects - Export

Cisco ISE Operations - System 360

Settings Monitoring **Log Analytics**

elastic Search Elastic

Stack Management Saved objects

Management

- Ingest
- Ingest Pipelines
- Alerts and Insights
- Rules and Connectors
- Kibana
- Index Patterns
- Saved Objects**
- Tags
- Advanced Settings

Saved Objects

Manage and share your saved objects. To edit the associated application.

Refresh Import Export 202 objects

Search...

Type Title

<input type="checkbox"/>	Advanced Settings [7.17.0]
<input checked="" type="checkbox"/>	RADIUS Authentication Summary
<input type="checkbox"/>	ISE Overview Dashboard
<input type="checkbox"/>	ISE Processes Summary
<input type="checkbox"/>	TACACS Authentication Summary
<input type="checkbox"/>	ISE Observability Dashboard
<input type="checkbox"/>	RADIUS Accounting Summary
<input type="checkbox"/>	TACACS Accounting Summary

That's because Log Analytics runs in an iframe

Reload

Bookmark Page...

Save Page As...

Save Page to Pocket

Select All

This Frame

View Page Source

Inspect Accessibility Properties

Inspect

Show Only This Frame

Open Frame in New Tab

Open Frame in New Window

Reload Frame

Bookmark Frame...

Save Frame As...

Print Frame...

Take Screenshot

View Frame Source

View Frame Info

Type Tags Delete Export

Actions

Log Analytics

Saved Objects – Export – Iframe Workaround

The screenshot shows the Cisco ISE Log Analytics interface. The top navigation bar includes 'Settings', 'Monitoring', and 'Log Analytics'. The main content area is titled 'Saved Objects' and contains a table of saved objects. An orange arrow points from a text overlay to the 'Advanced Settings [7.17.0]' link in the table. A context menu is open over the link, with 'Open Link in New Tab' selected.

As a workaround, right-click the menu and open in a new tab.

Type	Title	Tags	Actions
<input type="checkbox"/>	Advanced Settings [7.17.0]		
<input type="checkbox"/>	RADIUS Authentication Summary		
<input type="checkbox"/>	ISE Overview Dashboard		
<input type="checkbox"/>	ISE Processes Summary		
<input type="checkbox"/>	TACACS Authentication Summary		
<input type="checkbox"/>	ISE Observability Dashboard		
<input type="checkbox"/>	RADIUS Accounting Summary		
<input type="checkbox"/>	TACACS Accounting Summary		

Log Analytics

Saved Objects – Export – Iframe Workaround

The screenshot shows the Elastic Stack Management interface. The left sidebar contains the 'Management' section with links to 'Ingest', 'Alerts and Insights', 'Kibana', 'Index Patterns', 'Saved Objects', 'Tags', and 'Advanced Settings'. The main content area is titled 'Saved Objects' and shows a list of saved objects. A modal dialog is open for exporting a saved object, with the filename 'export.ndjson' entered. The dialog shows a list of files in the 'Downloads' folder. An orange arrow points to the 'Save' button in the modal, indicating the successful completion of the export process.

Enter name of file to save to...

Save As:

Tags:

Downloads

Name	Date Modified	Size
0Rj4aV7H.gz.part	11/21/22	
01_15_54.jpg	7/15/22	
02_19_02.jpg	5/5/23	
05_55_30.jpg	7/16/21	
5fa926884c855.jpg	4/6/23	
06_24_27.jpg	3/28/22	
06_53_46.jpg	7/16/21	
06_53_46(1).jpg	7/16/21	
08_47_08.jpg	10/22/21	
12_32_12.jpg	6/27/21	
172.31.255.73--9-30-21-155pm-M-CORE-1.pcapng	9/30/21	
172.31.255.73--9-30-21-155pm-M-CORE.pcapng	9/30/21	
1527_743_1.png	2/6/23	

Format: *.ndjson

New Folder Cancel Save

Refresh Import Export 202 objects

Type Tags Delete Export

Actions

Now the export is successful!

Log Analytics

Saved Objects - Import

Operations - System 360

Settings Monitoring **Log Analytics**

elastic Search Elastic

Stack Management Saved objects

Management

- Ingest [ⓘ]
Ingest Pipelines
- Alerts and Insights [ⓘ]
Rules and Connectors
- Kibana [ⓘ]
Index Patterns
Saved Objects
Tags
Advanced Settings

Saved Objects

Manage and share your saved objects. To edit the underlying data of an object, go to its associated application.

Search...

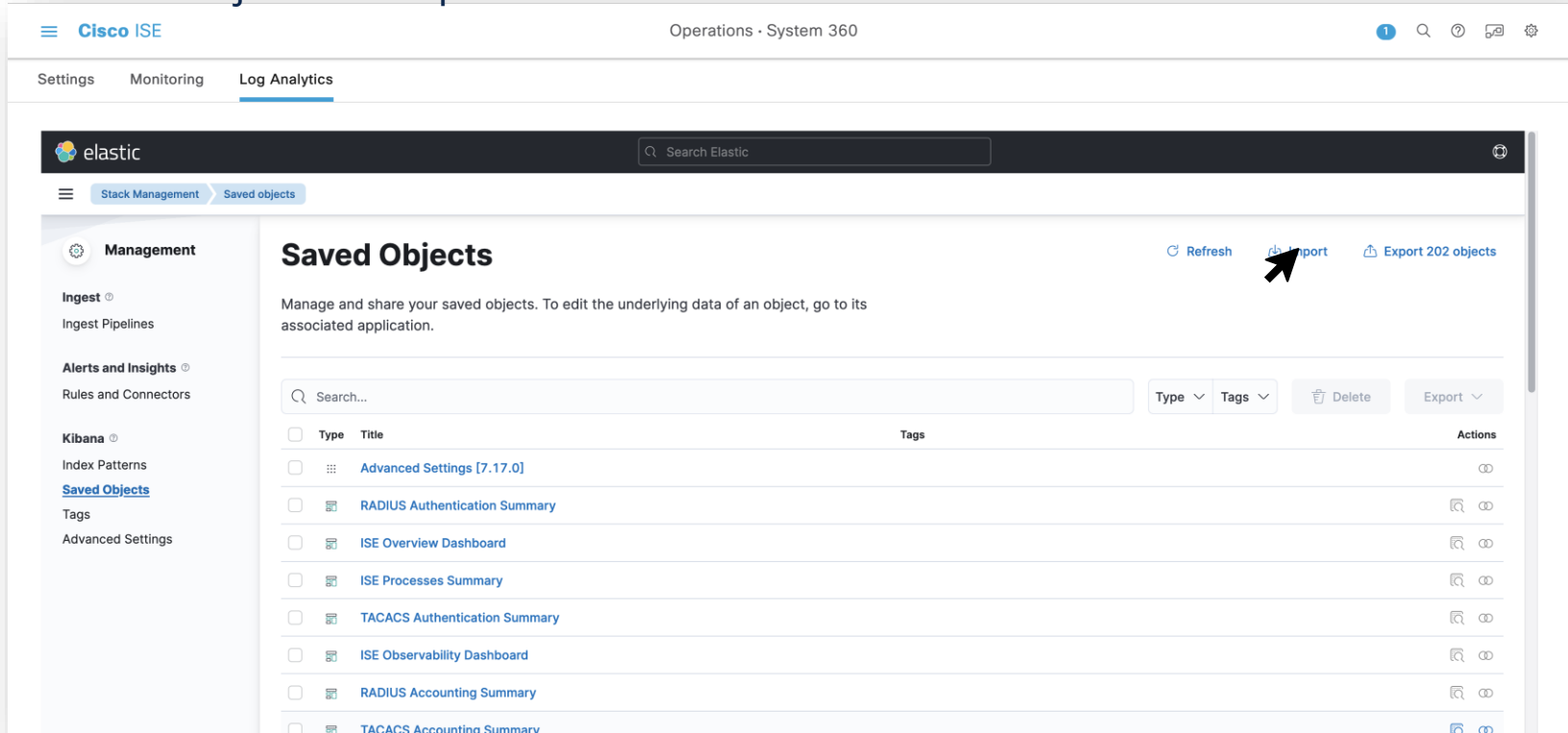
Type Tags Delete Export

Type	Title	Tags	Actions
<input type="checkbox"/>	Advanced Settings [7.17.0]		
<input type="checkbox"/>	RADIUS Authentication Summary		
<input type="checkbox"/>	ISE Overview Dashboard		
<input type="checkbox"/>	ISE Processes Summary		
<input type="checkbox"/>	TACACS Authentication Summary		
<input type="checkbox"/>	ISE Observability Dashboard		
<input type="checkbox"/>	RADIUS Accounting Summary		
<input type="checkbox"/>	TACACS Accounting Summary		

Import Export 202 objects

Log Analytics

Saved Objects - Import



The screenshot displays the Cisco ISE Log Analytics interface. At the top, the Cisco ISE logo is on the left, and 'Operations - System 360' is in the center. The right side of the top bar contains a notification icon, a search icon, a help icon, a chat icon, and a settings icon. Below the top bar, there are tabs for 'Settings', 'Monitoring', and 'Log Analytics'. The 'Log Analytics' tab is selected. The main content area is divided into two sections: 'Management' on the left and 'Saved Objects' on the right. The 'Management' section includes links for 'Ingest', 'Alerts and Insights', and 'Kibana'. The 'Saved Objects' section has a title 'Saved Objects' and a description: 'Manage and share your saved objects. To edit the underlying data of an object, go to its associated application.' Below this is a search bar and a table of saved objects. The table has columns for 'Type', 'Title', 'Tags', and 'Actions'. The 'Actions' column contains icons for 'Refresh', 'Import', and 'Export'. A black arrow points to the 'Import' button in the top right corner of the Elastic UI.

elastic Search Elastic

Stack Management Saved objects

Management

- Ingest[Ⓢ]
Ingest Pipelines
- Alerts and Insights[Ⓢ]
Rules and Connectors
- Kibana[Ⓢ]
Index Patterns
[Saved Objects](#)
Tags
Advanced Settings

Saved Objects

Manage and share your saved objects. To edit the underlying data of an object, go to its associated application.

Refresh Import Export 202 objects

Search...

Type Tags Delete Export

Type	Title	Tags	Actions
<input type="checkbox"/>	Advanced Settings [7.17.0]		
<input type="checkbox"/>	RADIUS Authentication Summary		
<input type="checkbox"/>	ISE Overview Dashboard		
<input type="checkbox"/>	ISE Processes Summary		
<input type="checkbox"/>	TACACS Authentication Summary		
<input type="checkbox"/>	ISE Observability Dashboard		
<input type="checkbox"/>	RADIUS Accounting Summary		
<input type="checkbox"/>	TACACS Accounting Summary		

Log Analytics

Saved Objects - Import

Import file selection

The screenshot shows the Cisco ISE Log Analytics interface. The top navigation bar includes 'Settings', 'Monitoring', and 'Log Analytics'. The main content area displays the 'Saved Objects' section with a list of objects. A modal dialog titled 'Import saved objects' is open on the right. The dialog has a section 'Select a file to import' with an 'Import' button. Below this is the 'Import options' section, which is highlighted with a red box. The 'Import options' section contains three radio buttons: 'Check for existing objects' (selected), 'Automatically overwrite conflicts', and 'Request action on conflict'. A green arrow points to the 'Import' button, and a red arrow points to the 'Import options' section.

Use caution as you could overwrite existing objects

Import options

- ☒ Check for existing objects
- ☐ Automatically overwrite conflicts
- ☐ Request action on conflict

Create new objects with random IDs

Log Analytics

Saved Objects - Import

Settings Monitoring Log Analytics

Operations - System 360



Settings Monitoring Log Analytics

elastic

Search Elastic

Stack Management Saved objects

Management

Ingest
Ingest Pipelines

Alerts and Insights
Rules and Connectors

Kibana
Index Patterns
Saved Objects
Tags
Advanced Settings

Saved Objects

Manage and share your saved objects. To edit the underlying data of an object, go to its associated application.

Search...

Type	Title
	Advanced Settings [7.17.0]
	RADIUS Authentication Summary
	ISE Overview Dashboard
	ISE Processes Summary
	TACACS Authentication Summary
	ISE Observability Dashboard
	RADIUS Accounting Summary
	TACACS Accounting Summary

Import saved objects

Select a file to import

Import

Import options

☒ Check for existing objects

☒ Automatically overwrite conflicts

☐ Request action on conflict

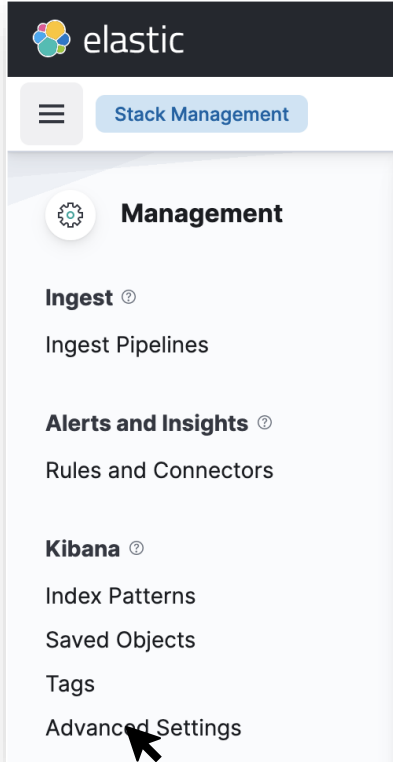
☐ Create new objects with random IDs

Using random IDs could lead to duplicate objects



Log Analytics

Menu – Advanced Settings



Log Analytics

Advanced Settings-Menu

The screenshot shows the Cisco ISE interface. At the top, the Cisco ISE logo is on the left, and 'Operations · System 360' is in the center. On the right, there's a status bar indicating 'Evaluation Mode 85 Days' along with search, help, and settings icons. Below this is a navigation bar with 'Settings', 'Monitoring', and 'Log Analytics' (which is selected). The main content area has a dark header with the 'elastic' logo and a search bar. Below the header, there's a 'Stack Management' tab and an 'Advanced Settings' tab. On the left, a 'Management' sidebar lists 'Ingest', 'Alerts and Insights', and 'Kibana', with 'Advanced Settings' highlighted. The main settings area is titled 'Settings' and includes a search bar and a 'Category' dropdown. A yellow caution box states: 'Caution: You can break stuff here. Be careful in here, these settings are for very advanced users only. Tweaks you make here can break large portions of Kibana. Some of these settings may be undocumented, unsupported or experimental. If a field has a default value, blanking the field will reset it to its default which may be unacceptable given other configuration directives. Deleting a custom setting will permanently remove it from Kibana's config.' The 'General' section contains three settings: 'Disable Batch Compression' (bfetch:disableCompression, Off), 'Quote CSV values' (csv:quoteValues, On), and 'CSV separator' (csv:separator, ,).

Cisco ISE Operations · System 360 Evaluation Mode 85 Days

Settings Monitoring Log Analytics

elastic Search Elastic

Stack Management Advanced Settings

Management

- Ingest
- Ingest Pipelines
- Alerts and Insights
- Rules and Connectors
- Kibana
- Index Patterns
- Saved Objects
- Tags
- [Advanced Settings](#)

Settings

Search... Category

Caution: You can break stuff here

Be careful in here, these settings are for very advanced users only. Tweaks you make here can break large portions of Kibana. Some of these settings may be undocumented, unsupported or experimental. If a field has a default value, blanking the field will reset it to its default which may be unacceptable given other configuration directives. Deleting a custom setting will permanently remove it from Kibana's config.

General

Disable Batch Compression

Disable batch compression. This allows you to debug individual requests, but increases response size.

bfetch:disableCompression ☐ Off

Quote CSV values

Should values be quoted in csv exports?

csv:quoteValues ☒ On

CSV separator

Separate exported values with this string

csv:separator

Log Analytics

Advanced Settings-Menu

The screenshot shows the Cisco ISE Log Analytics Advanced Settings menu. The left sidebar contains a 'Management' section with links to Ingest, Alerts and Insights, and Kibana. The main content area is titled 'Advanced Settings' and includes sections for 'Day of week', 'Scaled date format', 'Timezone for date formatting', 'Date with nanoseconds format', and 'Default index'. An annotation 'Allows you adjust the timezone displayed in the data' with an orange arrow points to the 'Timezone for date formatting' dropdown menu, which is open and shows a list of timezones with 'Browser' selected.

Operations · System 360

Settings Monitoring Log Analytics

elastic Search Elastic

Stack Management Advanced Settings

Management

Ingest
Ingest Pipelines

Alerts and Insights
Rules and Connectors

Kibana
Index Patterns
Saved Objects
Tags
[Advanced Settings](#)

Day of week
What day should weeks start on?

Scaled date format
Values that define the format used in situations where time-based data is rendered in order, and formatted timestamps should appear at the interval between measurements. Keys are [ISO8601 intervals](#).

Timezone for date formatting
Which timezone should be used. "Browser" will use the timezone detected by your browser.

Date with nanoseconds format
Used for the [date_nanos](#) datatype of Elasticsearch

Default index
The index to access if no index is set
Default: null

Browser

dateNanosFormat
MMM D, YYYY @ HH:mm:ss.SSSSSSSS

defaultIndex
15987767-d820-4b62-b904-4310262674da
[Reset to default](#)

Log Analytics

Advanced Settings-Menu

Cisco ISE Operations · System 360 Evaluation Mode 85 Days

Settings Monitoring **Log Analytics**

elastic Search Elastic

Stack Management Advanced Settings

Management

- Ingest [ⓘ]
 - Ingest Pipelines
- Alerts and Insights [ⓘ]
 - Rules and Connectors
- Kibana [ⓘ]
 - Index Patterns
 - Saved Objects
 - Tags
 - [Advanced Settings](#)

Shorten fields
Shorten long fields, for example, instead of foo.bar.baz, show f.b.baz

Sort options
[Options](#) for the Elasticsearch sort parameter

Store URLs in session storage
The URL can sometimes grow to be too large for some browsers to handle. To counter-act this we are testing if storing parts of the URL in session storage could help. Please let us know how it goes!

Dark mode
Enable a dark mode for the Kibana UI. A page refresh is required for the setting to be applied.

Theme version
Switch between the theme used for the current and next version of Kibana. A page refresh is required for the setting to be applied.

Time filter quick ranges
The list of ranges to show in the Quick section of the time filter. This should be an array of objects, with each object containing "from", "to" (see [accepted formats](#)), and "display" (the title to be

shortDots:enable
☐ Off

sort:options
`{ "unmapped_type": "boolean" }`

state:storeInSessionStorage
☐ Off

theme:darkMode
☐ Off

theme:version
v8

timepicker:quickRanges
`[{ "from": "now/d",`

Toggle dark mode

Log Analytics

Advanced Settings-Menu

The screenshot shows the Kibana Log Analytics Advanced Settings page. The left sidebar contains the following menu items: Management (selected), Ingest (with a sub-item Ingest Pipelines), Alerts and Insights (with a sub-item Rules and Connectors), and Kibana (with sub-items Index Patterns, Saved Objects, Tags, and Advanced Settings). The main content area is divided into several sections: Shorten fields (with a description and a toggle for shortDots.enable set to Off), Sort options (with a link to Elasticsearch sort parameter options and a text area for sort:options containing `{ "unmapped_type": "boolean" }`), Store URLs in session storage (with a description and a toggle for state:storeInSessionStorage set to Off), Dark mode (with a description and a toggle for theme:darkMode set to On), Theme version (with a description and a dropdown for theme:version set to v8), and Time filter quick ranges (with a description and a text area for timepicker:quickRanges containing an array of objects). A large orange arrow points from the text "Don't forget to save!" to the "Save changes" button at the bottom right. The bottom of the page features a dark bar with a notification "1 unsaved setting" on the left and "Cancel changes" and "Save changes" buttons on the right.

Don't forget to save!

Settings monitoring **Log Analytics**

Management

- Ingest Ingest Pipelines
- Alerts and Insights Rules and Connectors
- Kibana Index PatternsSaved ObjectsTags**Advanced Settings**

Shorten fields

Shorten long fields, for example, instead of foo.bar.baz, show f.b.baz

Sort options

[Options](#) for the Elasticsearch sort parameter

sort:options

```
{ "unmapped_type": "boolean" }
```

Store URLs in session storage

The URL can sometimes grow to be too large for some browsers to handle. To counteract this we are testing if storing parts of the URL in session storage could help. Please let us know how it goes!

Dark mode •

Enable a dark mode for the Kibana UI. A page refresh is required for the setting to be applied.

Theme version

Switch between the theme used for the current and next version of Kibana. A page refresh is required for the setting to be applied.

Time filter quick ranges

The list of ranges to show in the Quick section of the time filter. This should be an array of objects, with each object containing "from", "to" (see [accepted formats](#)), and "display" (the title to be displayed).

timepicker:quickRanges

```
[  
  {  
    "from": "now/d",  
    "to": "now/d",  
    "display": "Today"  
  },  
  {  
    "from": "now/w",  
    "to": "now/w",  
    "display": "This week"  
  }  
]
```

1 unsaved setting

Cancel changes Save changes

Demo



Thank You!

The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive