

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

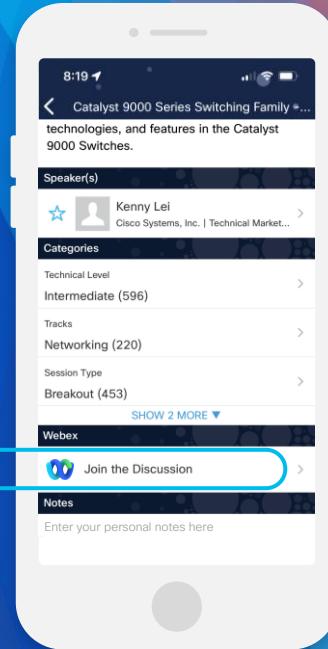
Questions?

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/ciscoalivebot/#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.



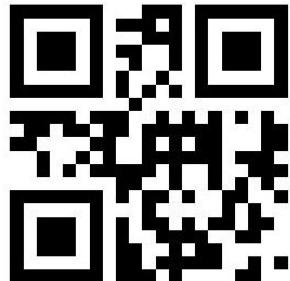
These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Cisco Live Challenge

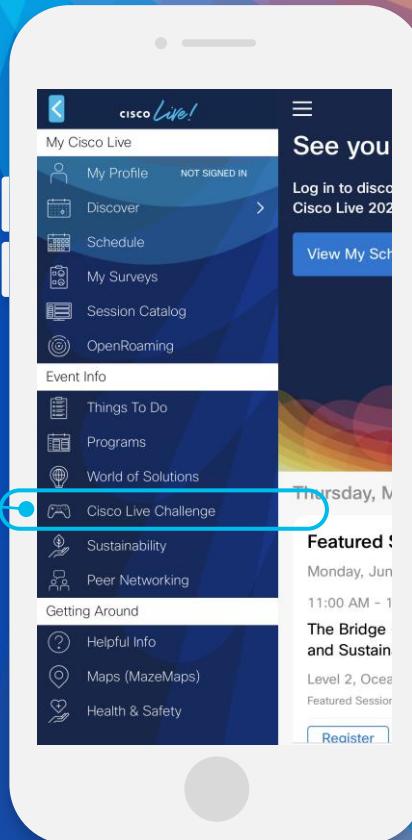
Gamify your Cisco Live experience!
Get points for attending this session!

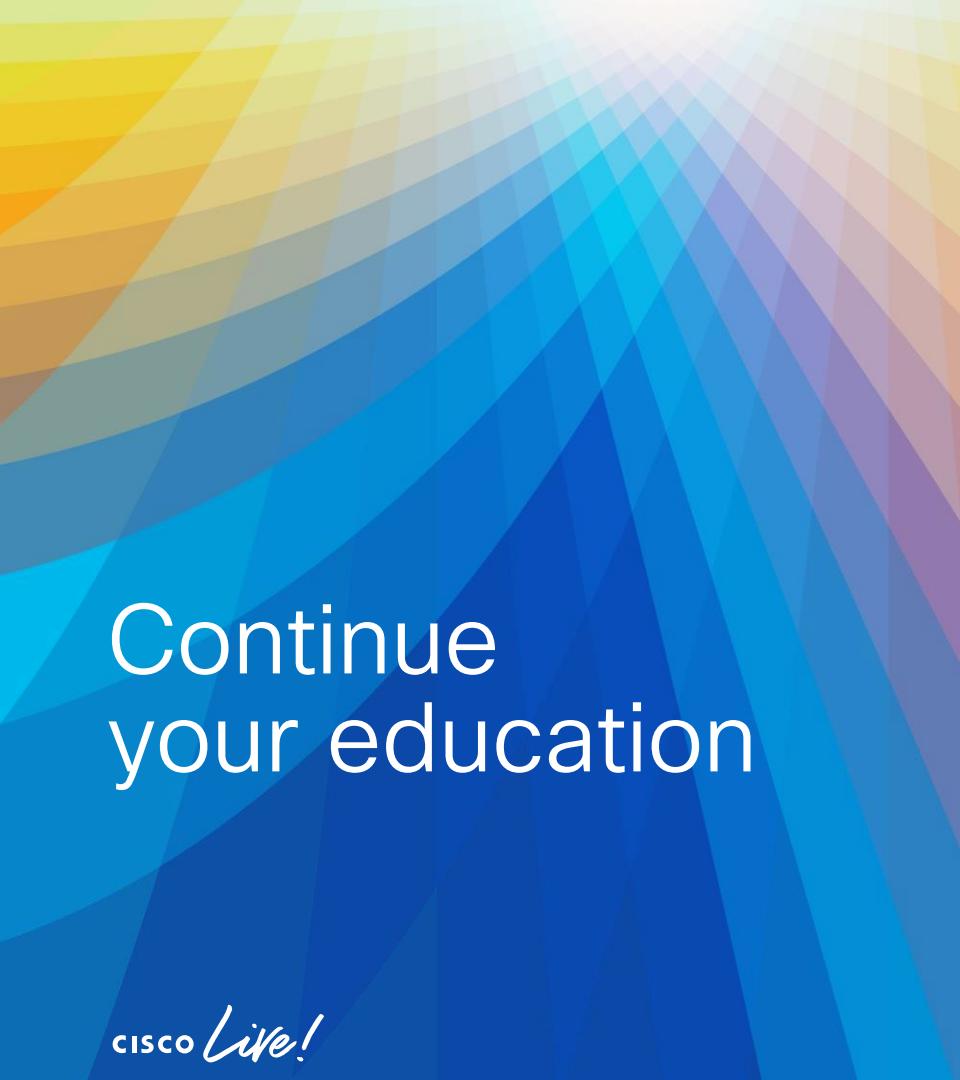
How:

- 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:



CISCO *Live!*





Continue your education

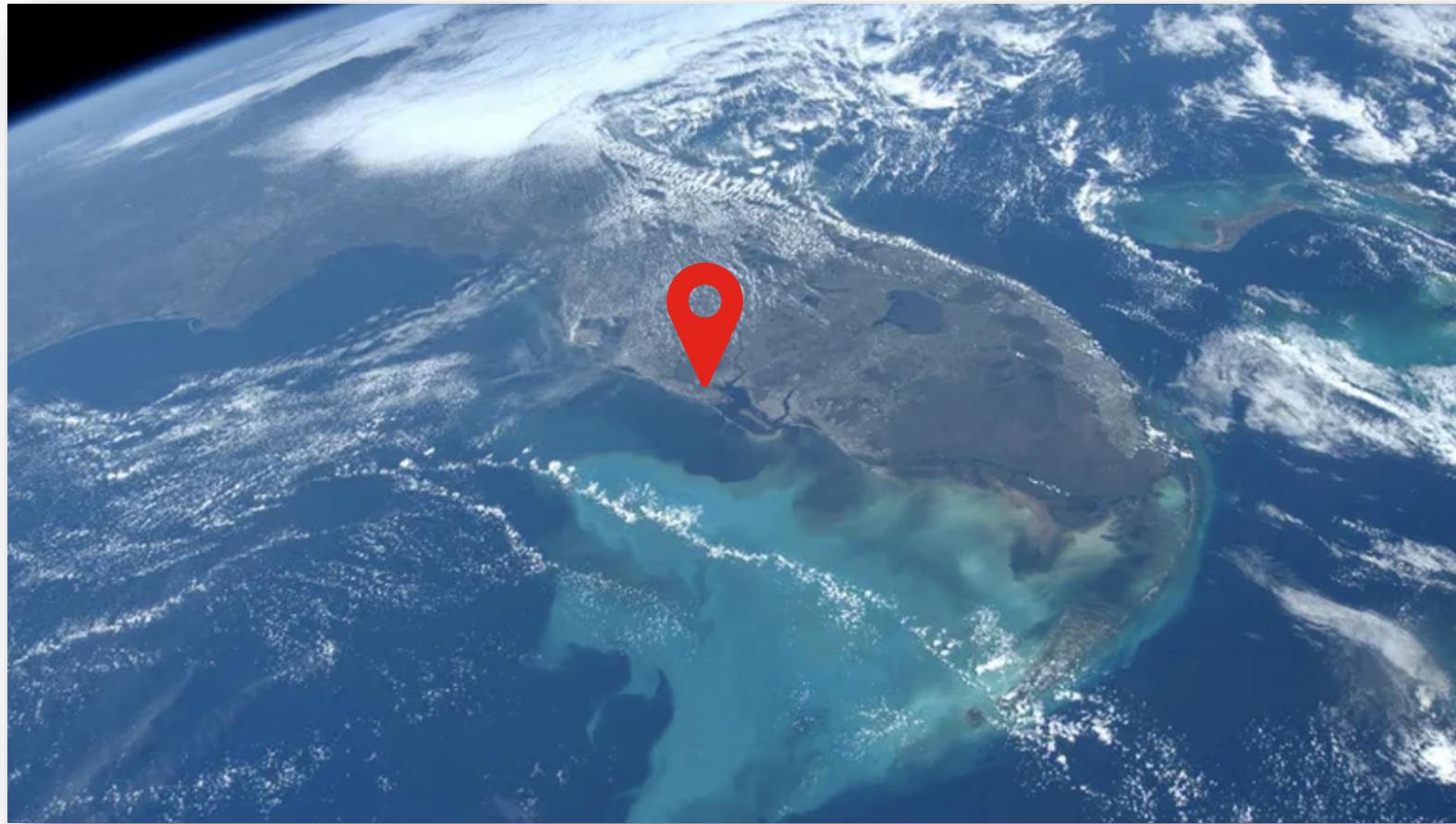
CISCO *Live!*

- 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 Needlesstack

- 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

 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](#) 

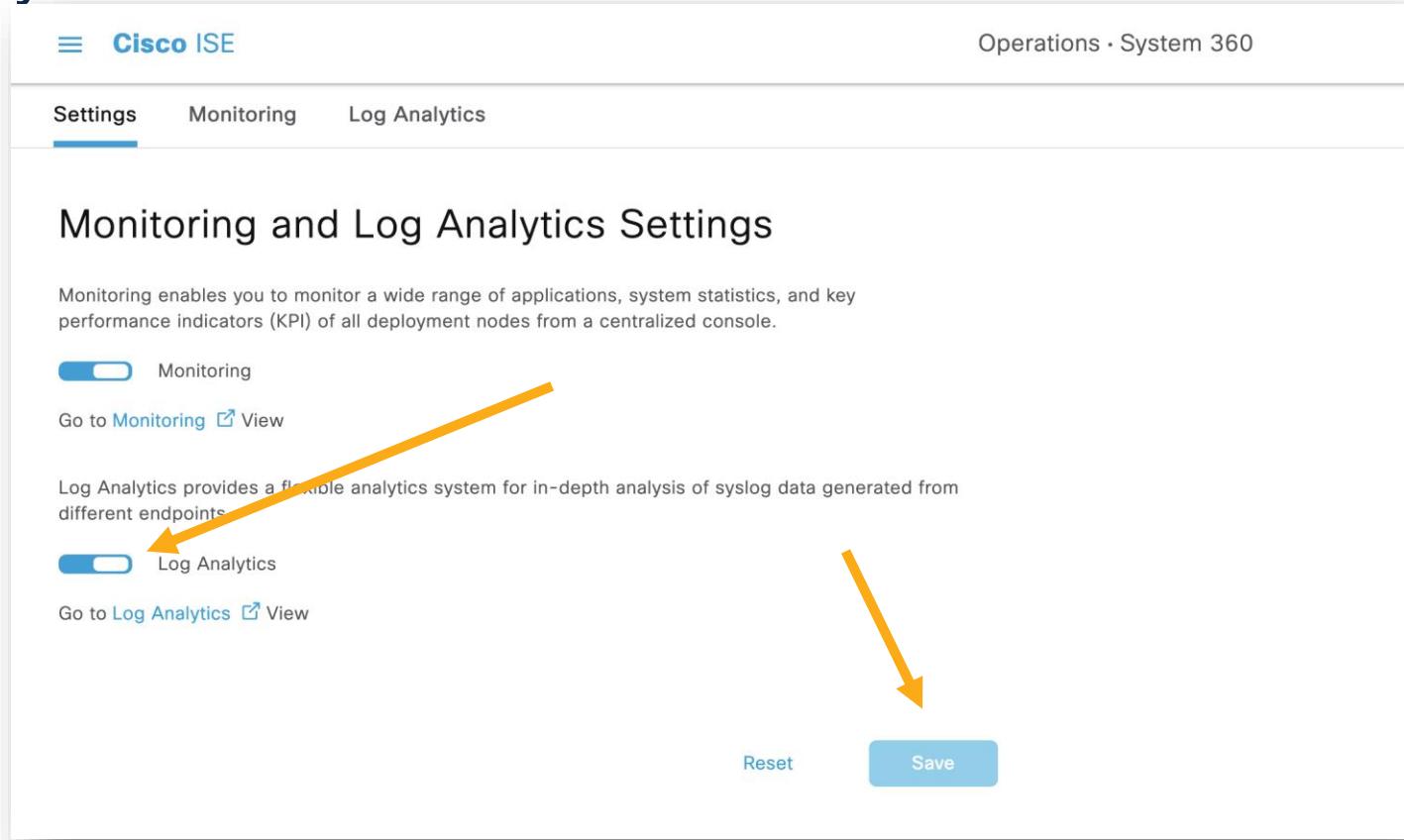
Log Analytics provides a flexible analytics system for in-depth analysis of syslog data generated from different endpoints.

 Log Analytics

Log Analytics

Enabling



The screenshot shows the Cisco ISE Settings page with the 'Monitoring' tab selected. The 'Monitoring' section is active, indicated by a blue underline. The 'Log Analytics' section is also present. Two orange arrows point from the text descriptions to their respective toggle buttons: one from 'Monitoring' to the 'Monitoring' toggle, and another from 'Log Analytics' to the 'Log Analytics' toggle. The 'Save' button is highlighted with a blue box.

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](#) 

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

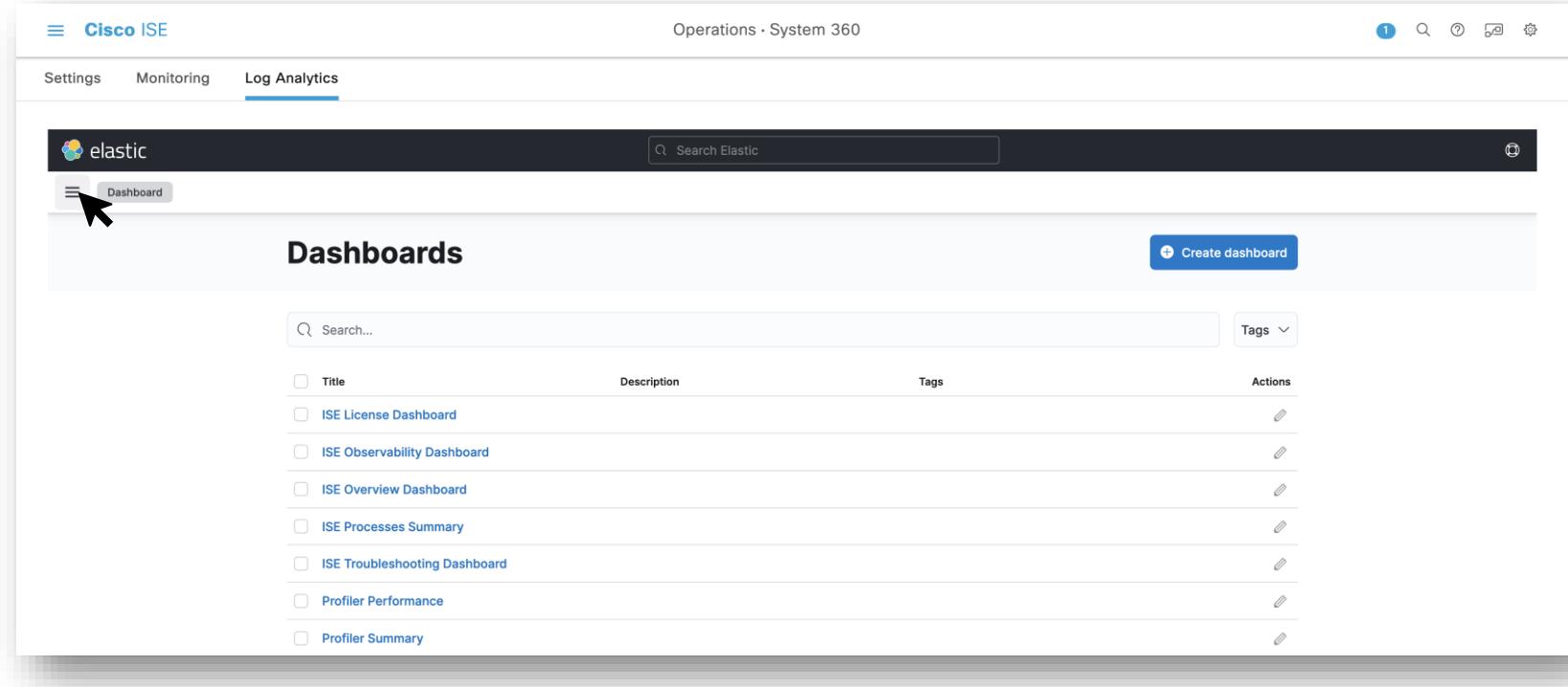
Log Analytics

Go to [Log Analytics](#) 

Reset Save

Log Analytics

Dashboards

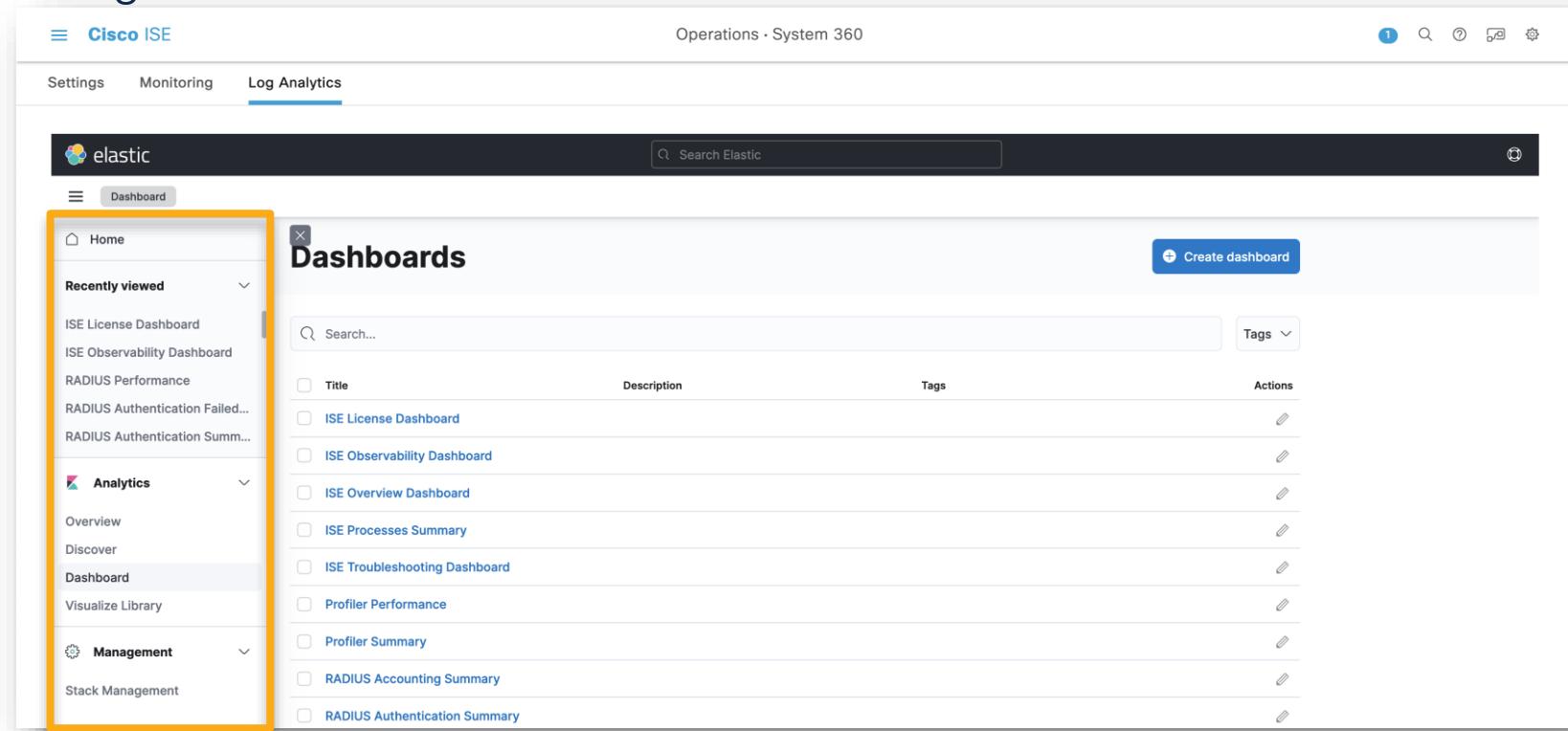


The screenshot shows the Cisco ISE Log Analytics Dashboards interface. The top navigation bar includes 'Cisco ISE', 'Operations · System 360', and various icons for search, refresh, and settings. Below the navigation is a sub-navigation bar with 'Settings', 'Monitoring', and 'Log Analytics' (which is underlined, indicating it is the active tab). The main content area is titled 'Dashboards' and features a 'Create dashboard' button. A search bar and a 'Tags' dropdown are also present. A list of dashboards is displayed, each with a title, description, tags, and an 'Actions' column with an edit icon. The dashboards listed are:

Title	Description	Tags	Actions
ISE License Dashboard			
ISE Observability Dashboard			
ISE Overview Dashboard			
ISE Processes Summary			
ISE Troubleshooting Dashboard			
Profiler Performance			
Profiler Summary			

Log Analytics

Navigation



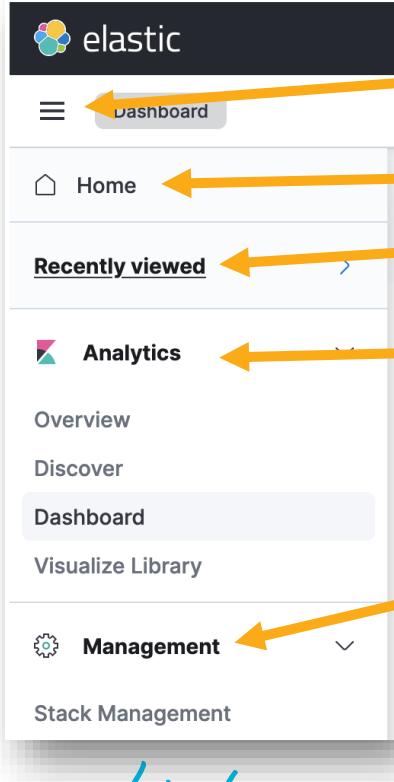
The screenshot shows the Cisco ISE Log Analytics interface. The top navigation bar includes the Cisco ISE logo, a search bar, and various system status indicators. Below the bar, a secondary navigation menu is visible with tabs for 'Settings', 'Monitoring', and 'Log Analytics', with 'Log Analytics' being the active tab. The main content area is titled 'Dashboards' and displays a list of available dashboards. A search bar and a 'Create dashboard' button are located at the top of this list. The list itself includes:

Title	Description	Tags	Actions
ISE License Dashboard			Edit
ISE Observability Dashboard			Edit
ISE Overview Dashboard			Edit
ISE Processes Summary			Edit
ISE Troubleshooting Dashboard			Edit
Profiler Performance			Edit
Profiler Summary			Edit
RADIUS Accounting Summary			Edit
RADIUS Authentication Summary			Edit

The left sidebar contains a 'Recently viewed' section and three main navigation categories: 'Analytics' (selected), 'Management', and 'Management'. The 'Analytics' category includes 'Overview', 'Discover', and 'Dashboard' (selected). The 'Management' category includes 'Stack Management'.

Log Analytics

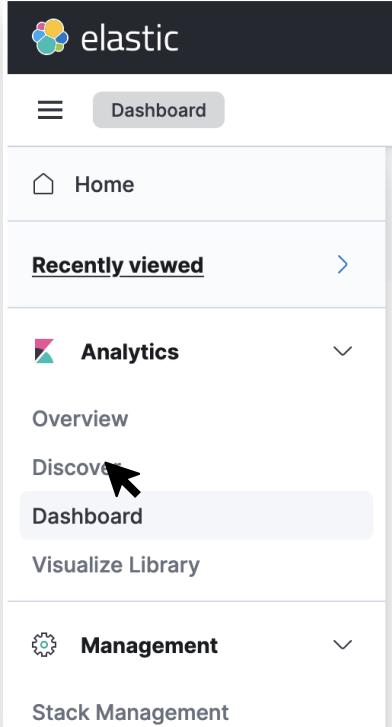
Navigation – Menus



- 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 shows the Cisco ISE Log Analytics Discover interface. The top navigation bar includes 'Cisco ISE', 'Operations - System 360', and various icons. Below the bar, the 'Log Analytics' tab is selected. The main area features a search bar with 'Search Elastic' and a 'Discover' button. On the left, a sidebar lists 'Selected fields' and 'Available fields' with a scroll bar. The main content area displays a histogram of log hits over time (May 10, 2023, 10:03:00 - 10:17:29.380) with a count of 82 hits. The histogram shows peaks around 10:08:00 and 10:11:00. Below the histogram is a table of log records. Annotations with orange arrows point to specific elements:

- Index Selection**: Points to the 'Selected fields' sidebar.
- Hit Count**: Points to the '82 hits' text.
- Time Range**: Points to the time range selector.
- Records**: Points to the table of log records.
- Available Fields**: Points to the 'Available fields' sidebar.

Log Analytics

Menu - Discover

Cisco ISE Operations - System 360

Settings Monitoring Log Analytics

elastic Search Elastic Options New Open Share Inspect Save Refresh

Discover

Search field names

Filter by type 0

Selected fields 1

Available fields 53

mnt_analytics_radius*

82 hits

Time acct_status_type

May 10, 2023 @ 10:02:29.380 - May 10, 2023 @ 10:17:29.380

Chart options

May 10, 2023 @ 10:16:59.983 -

May 10, 2023 @ 10:16:56.543 -

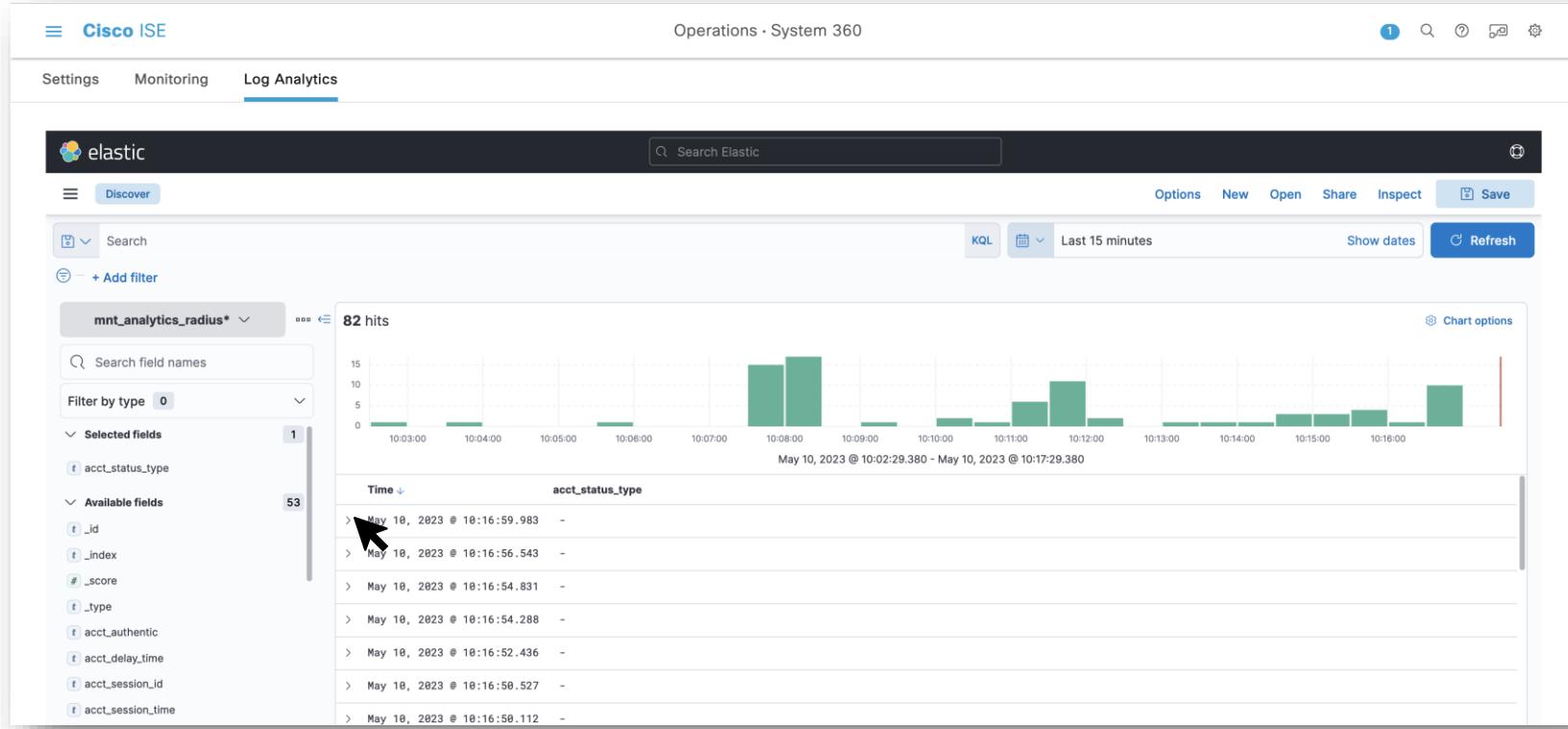
May 10, 2023 @ 10:16:54.831 -

May 10, 2023 @ 10:16:54.288 -

May 10, 2023 @ 10:16:52.436 -

May 10, 2023 @ 10:16:50.527 -

May 10, 2023 @ 10:16:50.112 -



Log Analytics

Menu - Discover

Cisco ISE Operations - System 360

Settings Monitoring Log Analytics

elastic Search Elastic Options New Open Share Inspect Save

Discover Search KQL Last 15 minutes Show dates Refresh

mnt_analytics_radius* 82 hits Chart options

Selected fields: acct_status_type

Filter by type: 0

Available fields: _id, _index, _score, _type, acct_authentic, acct_delay_time, acct_session_id, acct_session_time, acct_terminate_cause, acs_session_id

Time: May 10, 2023 @ 10:16:59.983

acct_status_type

Expanded document

Table JSON

Actions	Field	Value
	<code>t _id</code>	1JYFBogBYEq-UoX3_4XL
	<code>t _index</code>	mnt_analytics_radius_authentication-2023.05.10-000111
	<code># _score</code>	-
	<code>t _type</code>	_doc

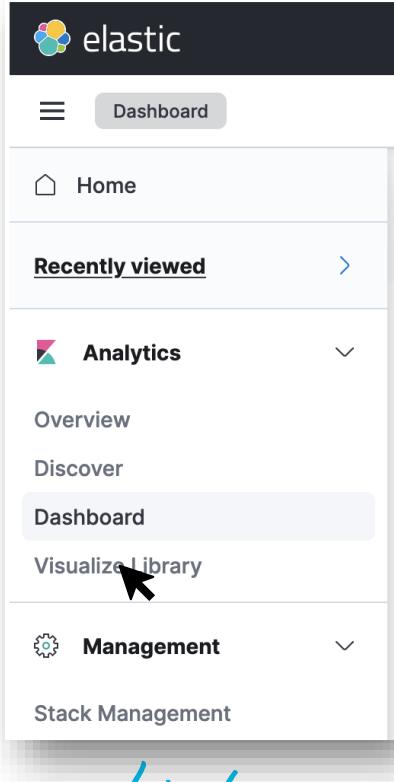
View surrounding documents View single document

Record Details

https://172.16.200.32/kibana/app/discover#/?_g=(filters:[{}],query:(language:kuery,query:"mnt_analytics_radius_authentication-2023.05.10-000111 _id:1JYFBogBYEq-UoX3_4XL _index:mnt_analytics_radius_authentication-2023.05.10-000111 _score:1 _type:doc")),sort:[{}],timeRange:(from:now-15m, to:now),timeZone:(auto),version:1

Log Analytics

Navigation – Menus

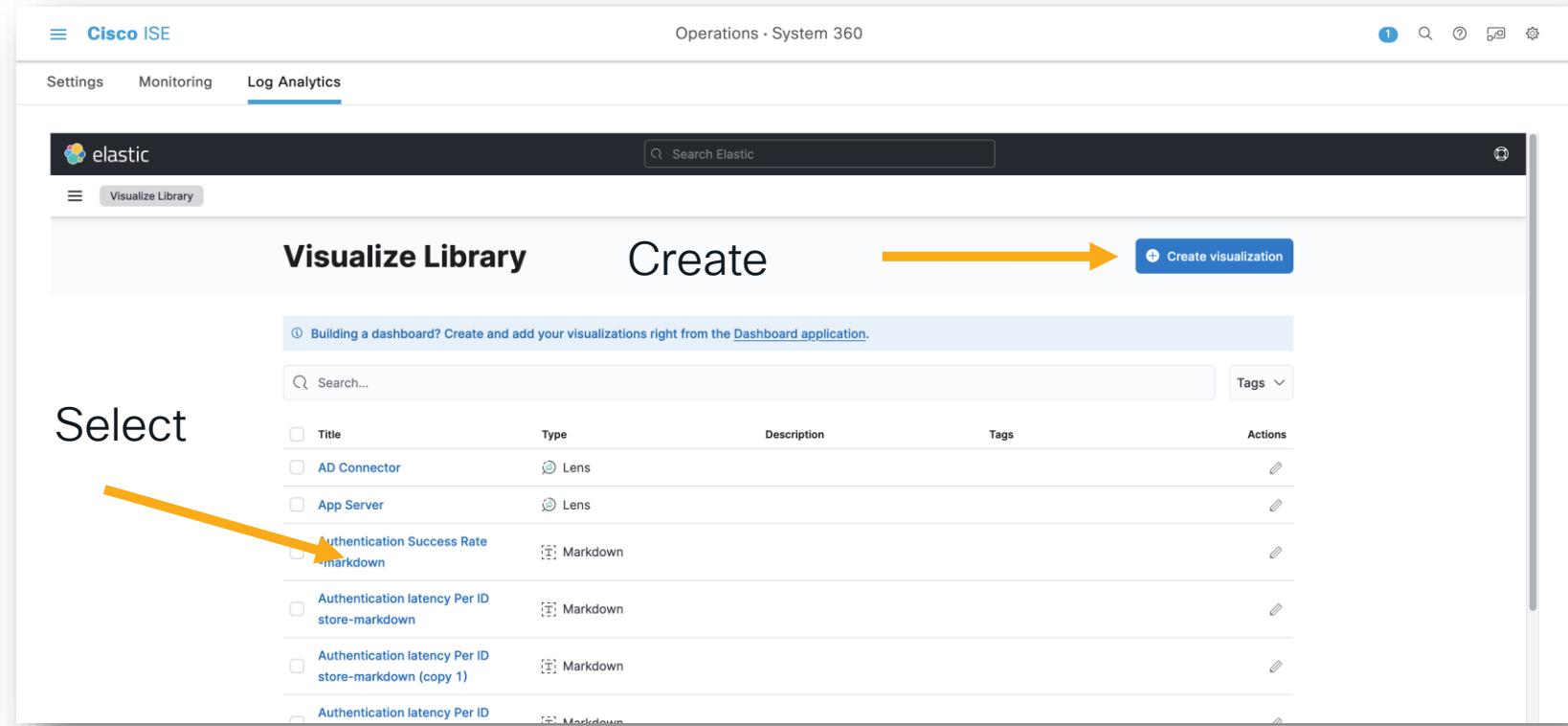


elastic

- Dashboard
- Home
- Recently viewed >
- Analytics** ▾
 - Overview
 - Discover
 - Dashboard**
 - Visualize Library** 
- Management** ▾
 - Stack Management

Log Analytics

Menu - Visualizations



Operations - System 360

Cisco ISE

Settings Monitoring Log Analytics

elastic

Search Elastic

Visualize Library

Visualize Library Create

Building a dashboard? Create and add your visualizations right from the Dashboard application.

Select

<input type="checkbox"/> 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"/> -markdown				
<input type="checkbox"/> Authentication latency Per ID	Markdown			
<input type="checkbox"/> store-markdown				
<input type="checkbox"/> Authentication latency Per ID	Markdown			
<input type="checkbox"/> store-markdown (copy 1)				
<input type="checkbox"/> Authentication latency Per ID	Markdown			
<input type="checkbox"/> store-markdown				

Create visualization

Log Analytics

Visualizations - Create

Cisco ISE Operations - System 360

Settings Monitoring Log Analytics

elastic Search Elastic

Visualize Library

Visualize Library

Create visualization

Building a dashboard? Create and add your visualizations right from the Dashboard application.

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			

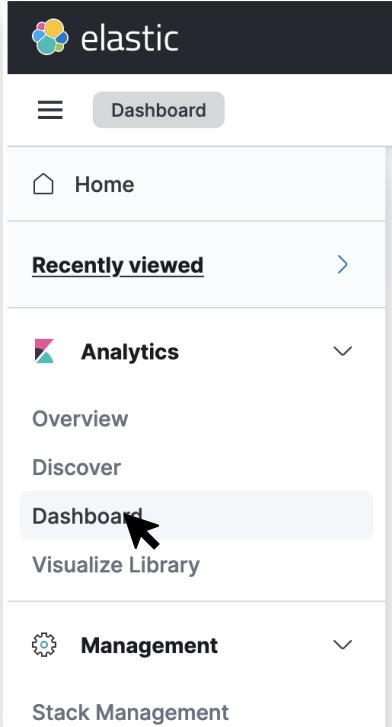
Log Analytics

Visualizations - Create

The screenshot shows the Cisco ISE Log Analytics interface. The top navigation bar includes 'Cisco ISE', 'Operations - System 360', and various icons. The 'Log Analytics' tab is selected. On the left, a sidebar titled 'Visualize I...' lists various log types: 'Building a dashboard', 'Search...', 'Title', 'AD Connector', 'App Server', 'Authentication Success - markdown', 'Authentication late store-markdown', 'Authentication late store-markdown (c...', 'Authentication late store-markdown (c...', and 'Authentications By...'. A 'Visualize Library' button is also present. The main content area is a 'New visualization' dialog box. It contains several sections: 'Lens' (described as a drag-and-drop editor for most users), 'TSVB' (described as advanced analysis for time series data), 'Custom visualization' (using Vega syntax), 'Aggregation based' (using a classic visualization library for charts), and 'Tools' (Text and Controls). Below the dialog, a 'Want to learn more?' link points to 'Read documentation'.

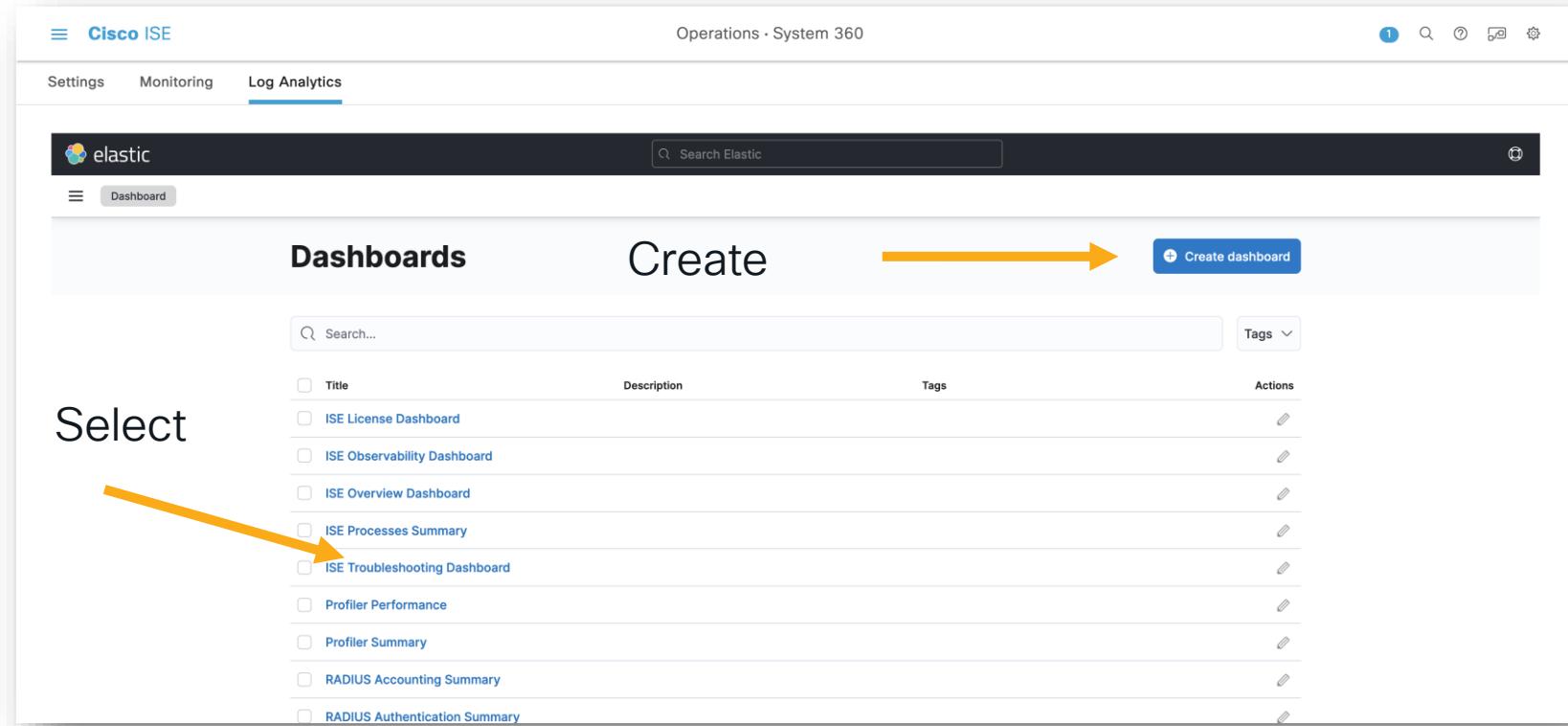
Log Analytics

Navigation – Menus



Log Analytics

Menu - Dashboards

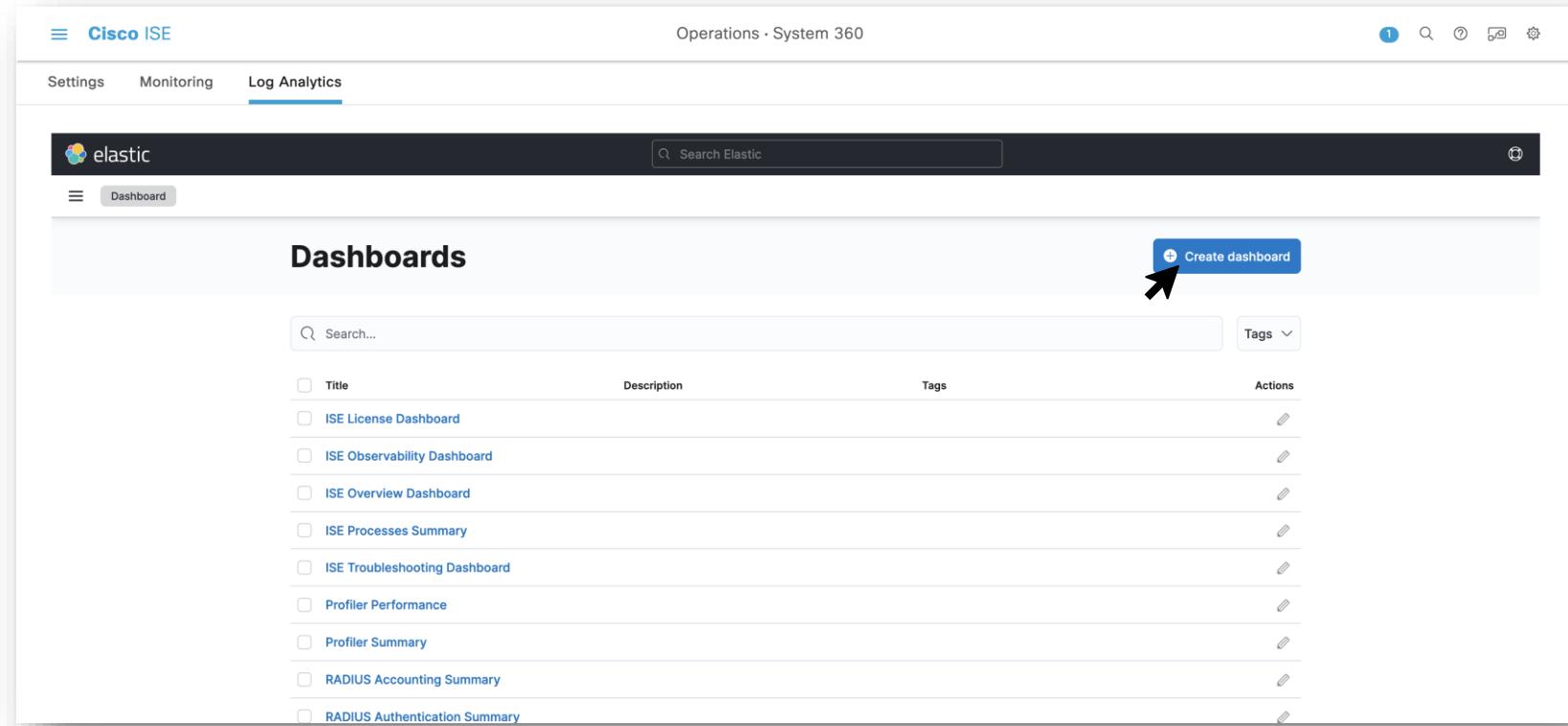


The screenshot shows the Cisco ISE Log Analytics interface. At the top, there is a navigation bar with 'Cisco ISE' and 'Operations - System 360'. Below the navigation bar, there are three tabs: 'Settings', 'Monitoring', and 'Log Analytics', with 'Log Analytics' being the active tab. The main content area is titled 'Dashboards' and 'Create'. A 'Create dashboard' button is located on the right. Below this, there is a search bar and a 'Tags' dropdown. A list of dashboard options is shown, with the 'ISE Troubleshooting Dashboard' highlighted by a yellow arrow. The list includes:

<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

Dashboards - Create

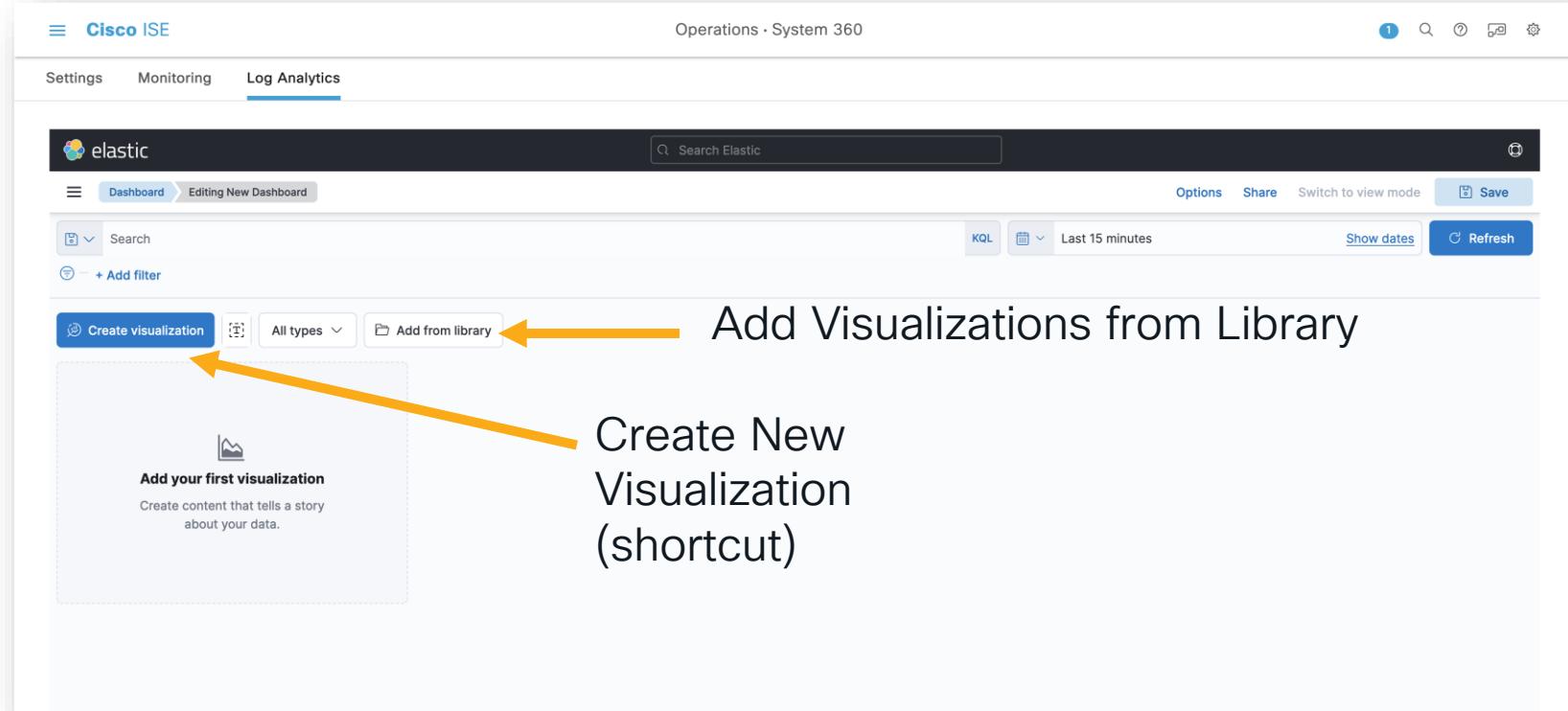


The screenshot shows the Cisco ISE Log Analytics interface. At the top, there is a navigation bar with the Cisco ISE logo, the text "Operations - System 360", and several icons. Below the navigation bar, there is a sub-navigation bar with "Settings", "Monitoring", and "Log Analytics" tabs, where "Log Analytics" is currently selected. The main content area is titled "Dashboards" and contains a search bar and a "Create dashboard" button. Below the search bar is a table with columns for "Title", "Description", "Tags", and "Actions". The table lists several dashboard templates, each with a checkbox and an edit icon in the "Actions" column. A mouse cursor is pointing at the "Create dashboard" button.

Title	Description	Tags	Actions
ISE License Dashboard			
ISE Observability Dashboard			
ISE Overview Dashboard			
ISE Processes Summary			
ISE Troubleshooting Dashboard			
Profiler Performance			
Profiler Summary			
RADIUS Accounting Summary			
RADIUS Authentication Summary			

Log Analytics

Dashboards - Create



Cisco ISE Operations - System 360

Settings Monitoring Log Analytics

elastic Search Elastic

Dashboard Editing New Dashboard Options Share Switch to view mode Save

Search All types Add from library

+ Add filter KQL Last 15 minutes Show dates Refresh

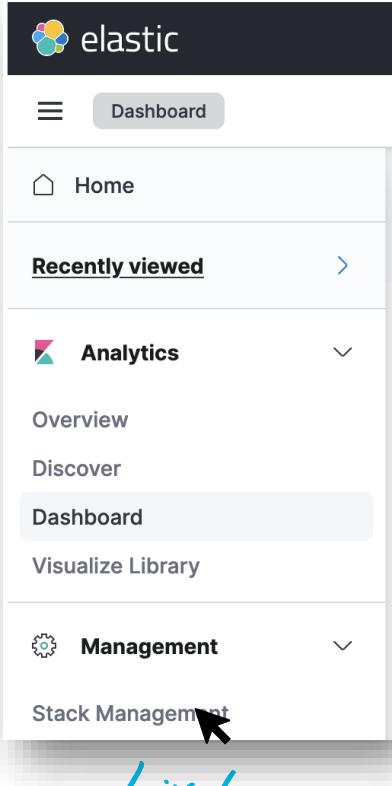
Create visualization Add your first visualization Create content that tells a story about your data.

Add Visualizations from Library

Create New Visualization (shortcut)

Log Analytics

Navigation – Menus



elastic

Dashboard

Home

Recently viewed >

Analytics ▾

- Overview
- Discover
- Dashboard**
- Visualize Library

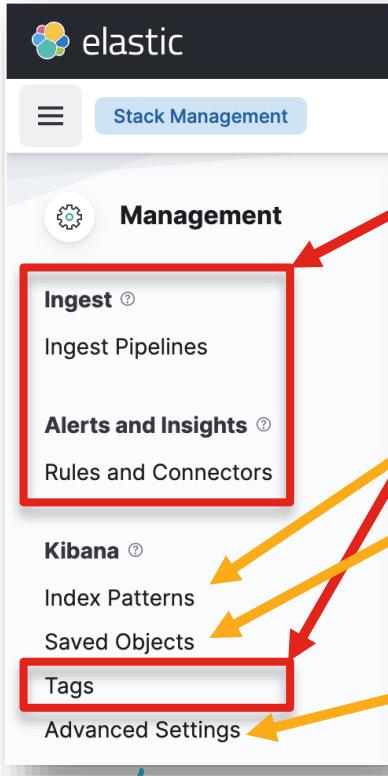
Management ▾

- Stack Management** 

CISCO Live!

Log Analytics

Menus – Stack Management



Not currently supported

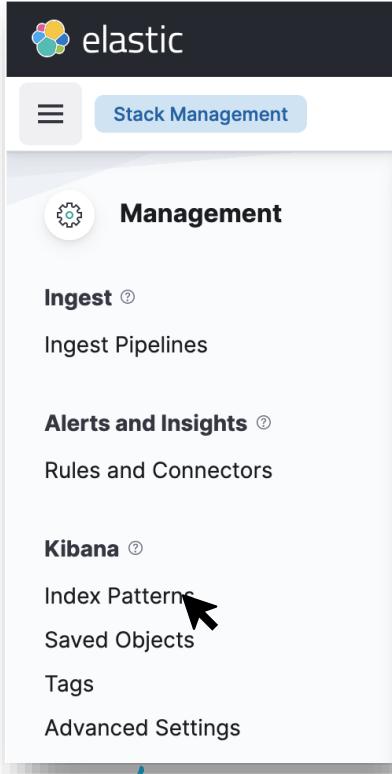
Kibana index search patterns

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

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

Log Analytics

Menu - Index Patterns



The screenshot shows the 'Management' section of the Elastic Stack interface. The 'Index Patterns' option is highlighted with a black arrow pointing to it. The interface includes a top navigation bar with the 'elastic' logo and 'Stack Management' tab, and a sidebar with 'Management', 'Ingest', 'Alerts and Insights', 'Kibana', and 'Advanced Settings' sections.

- Management
- Ingest ②
- Ingest Pipelines
- Alerts and Insights ②
- Rules and Connectors
- Kibana ②
- Index Patterns (selected)
- Saved Objects
- Tags
- Advanced Settings

Log Analytics

Menu - Index Patterns

The screenshot shows the Cisco ISE Log Analytics interface. The top navigation bar includes 'Cisco ISE', 'Operations - System 360', and various search and filter icons. Below the bar, the 'Log Analytics' tab is selected. The main content area is titled 'Index patterns' and contains a sub-header 'Create and manage the index patterns that help you retrieve your data from Elasticsearch.' A search bar is present. On the left, a sidebar lists 'Management' (Ingest, Alerts and Insights, Kibana), 'Index Patterns' (Index Patterns, Saved Objects, Tags, Advanced Settings), and 'Logs' (Logs, Log Sources, Log Types, Log Fields). A list of index patterns is displayed, including: 'mnt_analytics_tacacs_authentication*' (Default), 'mnt_analytics*', 'mnt_analytics_ise_counters*', 'mnt_analytics_license_counters*', 'mnt_analytics_process_status*', 'mnt_analytics_profiler_profiled*', and 'mnt_analytics_radius*'. A 'Create index pattern' button is located in the top right of the main content area.

Log Analytics

Index Patterns - Create

The screenshot shows the Cisco ISE Log Analytics interface for creating index patterns in the Elastic Stack Management section. The top navigation bar includes 'Cisco ISE', 'Operations - System 360', and various search and filter icons. Below the navigation is a secondary navigation bar with 'Settings', 'Monitoring', and 'Log Analytics' tabs, where 'Log Analytics' is selected. The main content area is titled 'Index patterns' and contains a sub-header 'Management'. A search bar labeled 'Search Elastic' is present. On the right, a blue button labeled '+ Create index pattern' is highlighted with a large black arrow pointing to it. The left sidebar lists categories: 'Ingest', 'Alerts and Insights', 'Kibana', and 'Index Patterns'. Under 'Index Patterns', 'Saved Objects', 'Tags', and 'Advanced Settings' are listed. A list of index patterns is shown, including 'mnt_analytics_tacacs_authentication*', 'Default', 'mnt_analytics*', 'mnt_analytics_ise_counters*', 'mnt_analytics_license_counters*', 'mnt_analytics_process_status*', 'mnt_analytics_profiler_profiled*', and 'mnt_analytics_radius*'. The 'Index Patterns' section is also highlighted with a blue box and a black arrow.

Log Analytics

Index Patterns - Create

Kibana index search pattern

Select a timestamp field

Indexes matched by pattern

Create index pattern

Name: mnt*

Use an asterisk (*) to match multiple characters. Spaces and the characters , /, ?, <, >, | are not allowed.

Timestamp field

Select a timestamp field

@timestamp
event_timestamp
logged_at
logged_at_timezone

--- I don't want to use the time filter ---

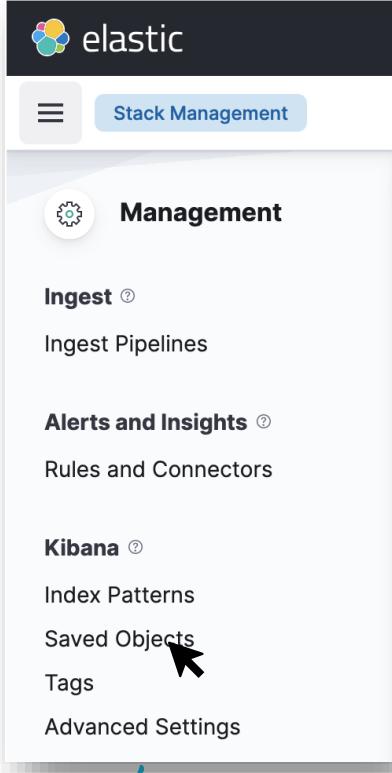
✓ Your index pattern matches 80 sources.

Index Pattern	Type
mnt_analytics_ise_counters	Alias
mnt_analytics_ise_counters-2023.05.05-000106	Index
mnt_analytics_ise_counters-2023.05.06-000107	Index
mnt_analytics_ise_counters-2023.05.07-000108	Index
mnt_analytics_ise_counters-2023.05.08-000109	Index
mnt_analytics_ise_counters-2023.05.09-000110	Index
mnt_analytics_ise_counters-2023.05.10-000111	Index
mnt_analytics_ise_counters-2023.05.11-000112	Index
mnt_analytics_license_counters	Alias
mnt_analytics_license_counters-2023.05.04-000010	Index

Rows per page: 10

Log Analytics

Menu - Saved Objects



The screenshot shows the 'Management' section of the Elastic Stack Management interface. The 'Saved Objects' item is highlighted with a black cursor icon pointing to it. The interface includes a navigation bar with 'elastic' and 'Stack Management' buttons, and a sidebar with 'Management', 'Ingest', 'Alerts and Insights', 'Kibana', and 'Advanced Settings' sections.

- Management
- Ingest ②
- Ingest Pipelines
- Alerts and Insights ②
- Rules and Connectors
- Kibana ②
- Index Patterns
- Saved Objects** 
- Tags
- Advanced Settings

Log Analytics

Saved Objects - Menu

The screenshot shows the Cisco ISE Log Analytics interface within the Elastic Stack. The top navigation bar includes 'Cisco ISE', 'Operations - System 360', and various search and filter icons. Below the bar, the 'Log Analytics' tab is selected. The main content area is titled 'Saved Objects' and displays a list of saved objects. The left sidebar contains navigation links for 'Management', 'Ingest', 'Alerts and Insights', 'Kibana', and 'Saved Objects' (which is currently selected). The main table lists the following saved objects:

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

Log Analytics

Saved Objects - Export

Operations - System 360

Cisco ISE

Settings Monitoring Log Analytics

elastic

Stack Management Saved objects

Management

Ingest

Alerts and Insights

Kibana

Saved Objects

Tags

Advanced Settings

Search Elastic

Refresh Import Export 202 objects

Select individual objects or export all

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		

Search...

Type Tags Delete Export

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

Log Analytics

Saved Objects - Export

Cisco ISE Operations - System 360

Settings Monitoring Log Analytics

elasticsearch Stack Management Saved objects

Management Ingest Alerts and Insights Kibana

Saved Objects

Saved Objects

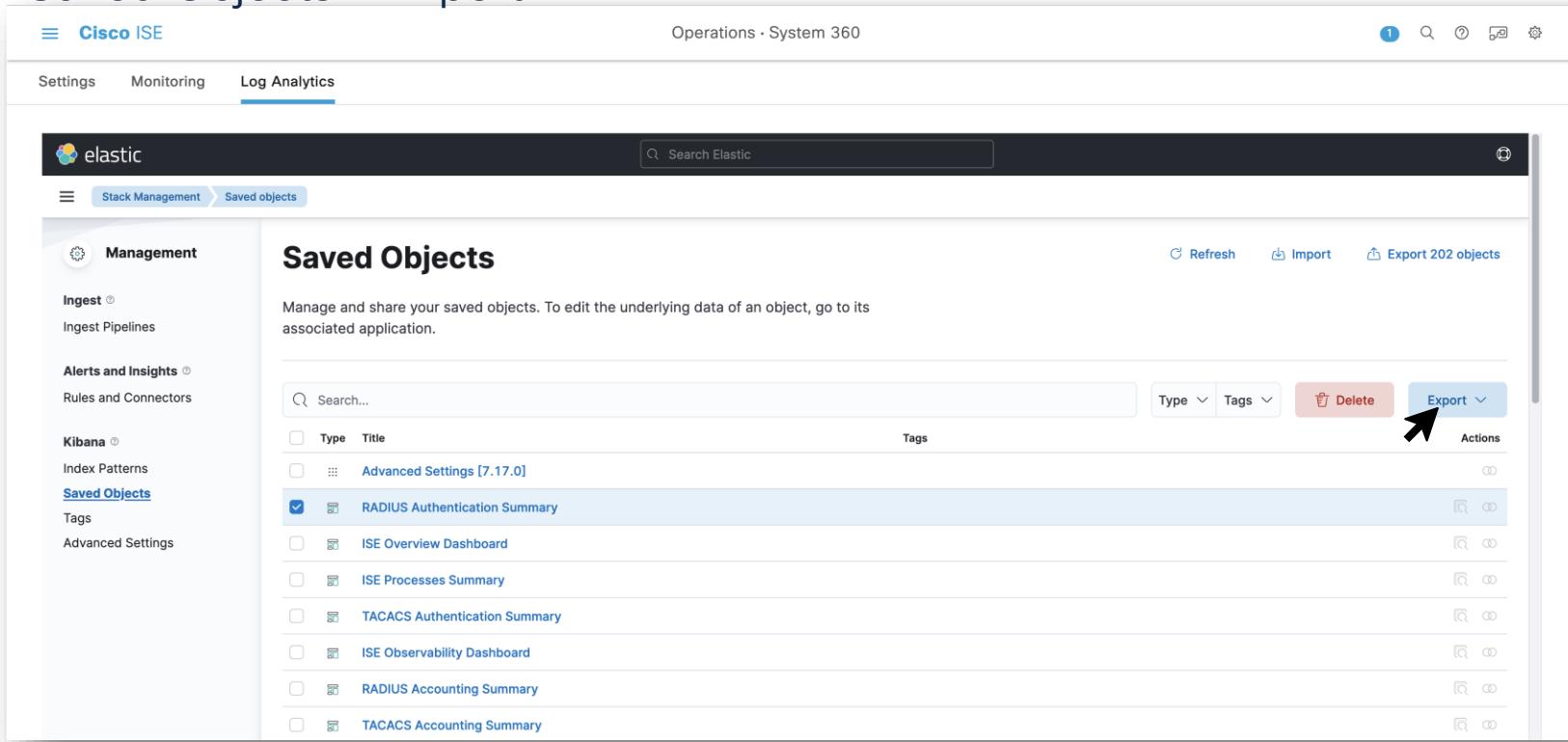
Manage and share your saved objects. To edit the underlying data of an object, go to its associated application.

Search... Type Tags Delete Export

Type	Title	Tags	Actions
Advanced Settings [7.17.0]	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		

Log Analytics

Saved Objects - Export



The screenshot shows the Cisco ISE Log Analytics interface. The top navigation bar includes 'Cisco ISE', 'Operations - System 360', and various icons. Below the navigation is a secondary navigation bar with 'Settings', 'Monitoring', and 'Log Analytics' (which is underlined). The main content area is titled 'Saved Objects' and includes a sub-navigation bar with 'Stack Management' and 'Saved objects'. On the left, a sidebar lists 'Management' (Ingest, Alerts and Insights, Kibana), 'Saved Objects' (Index Patterns, Tags, Advanced Settings), and 'Saved Objects' (under 'Management'). The main table lists various saved objects with columns for 'Type', 'Title', and 'Tags'. The 'Actions' column contains icons for search, copy, and delete. A red arrow points to the 'Export' button in the 'Actions' column of the table header.

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 Stack Management Saved objects

Search Elastic

Saved Objects

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

Choose to include dependencies

Refresh Import Export 202 objects

Search... Type Tags Delete Export

Options Include related objects Export

Type Title

Advanced Settings [7.17.0]

RADIUS Authentication Summary

ISE Overview Dashboard

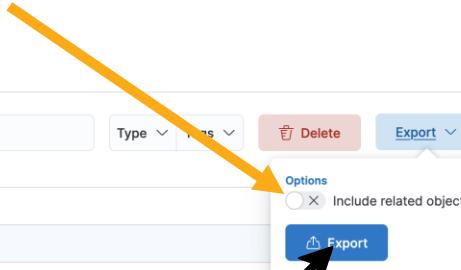
ISE Processes Summary

TACACS Authentication Summary

ISE Observability Dashboard

RADIUS Accounting Summary

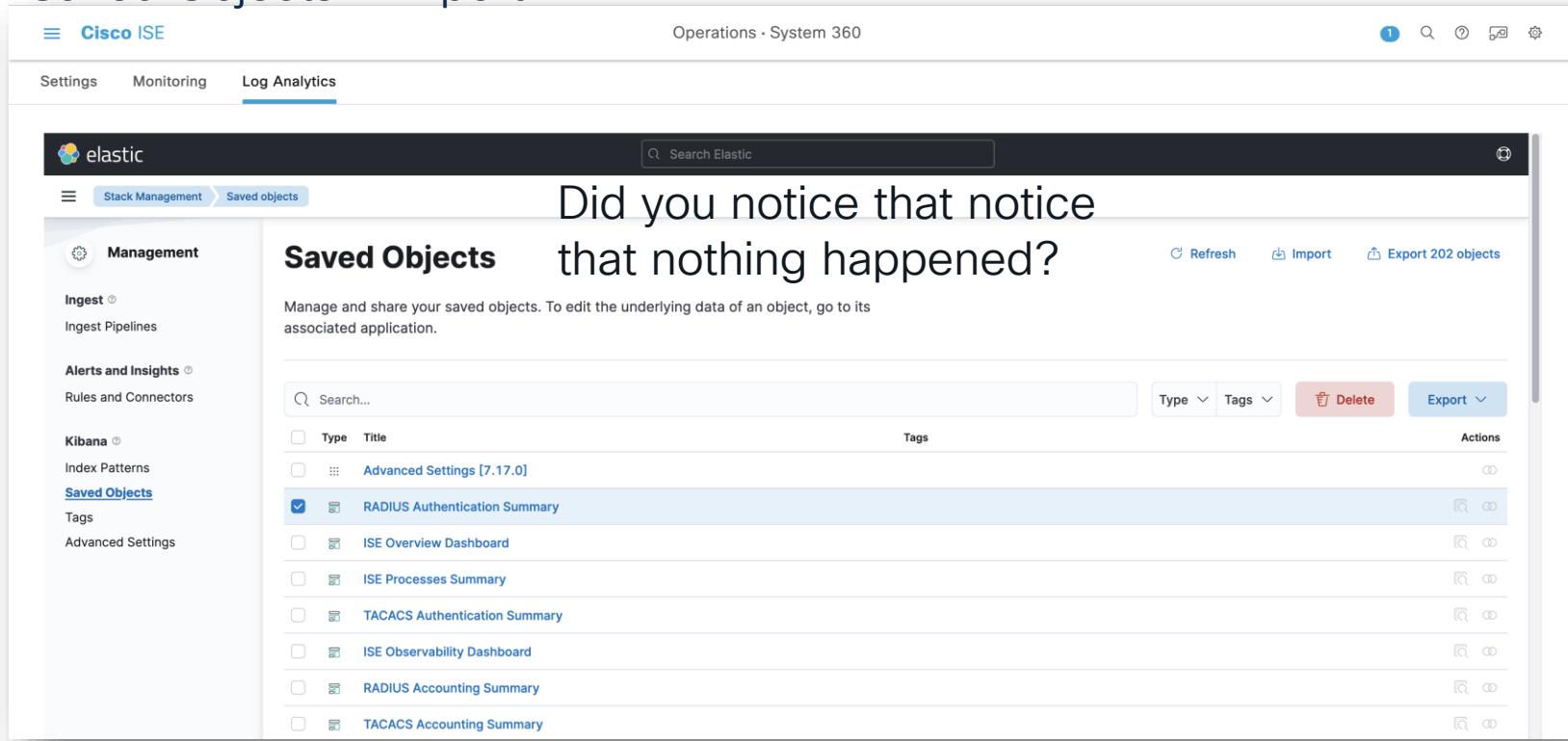
TACACS Accounting Summary



CISCO Live! #CiscoLive BRKSEC-2897 © 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public 55

Log Analytics

Saved Objects - Export



Operations - System 360

Cisco ISE

Settings Monitoring Log Analytics

elastic

Search Elastic

Stack Management Saved objects

Management

Ingest ②
Ingest Pipelines

Alerts and Insights ②
Rules and Connectors

Kibana ②
Index Patterns
Saved Objects
Tags
Advanced Settings

Did you notice that notice
that nothing happened?

Refresh Import Export 202 objects

Search...

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 'Cisco ISE', 'Operations - System 360', and various search and settings icons. Below the navigation is a secondary navigation bar with 'Settings', 'Monitoring', and 'Log Analytics' tabs, where 'Log Analytics' is selected. The main content area is titled 'Saved Objects' and contains a list of saved objects. A context menu is open over the first item in the list, 'RADIUS Authentication Summary'. The menu is titled 'This Frame' and includes options like 'Reload', 'Bookmark Page...', 'Save Page As...', 'Save Page to Pocket', 'Select All', 'View Page Source', 'Inspect Accessibility Properties', and 'Inspect'. To the right of the menu, there are buttons for 'Refresh', 'Import', and 'Export 202 objects'. The bottom of the interface features a 'Actions' section with icons for each object in the list.

That's because Log Analytics runs in an iframe

Operations - System 360

Cisco ISE

Settings Monitoring Log Analytics

elastic

Stack Management Saved objects

Management

Ingest

Alerts and Insights

Kibana

Saved Objects

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

Search...

Actions

Refresh Import Export 202 objects

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

Actions

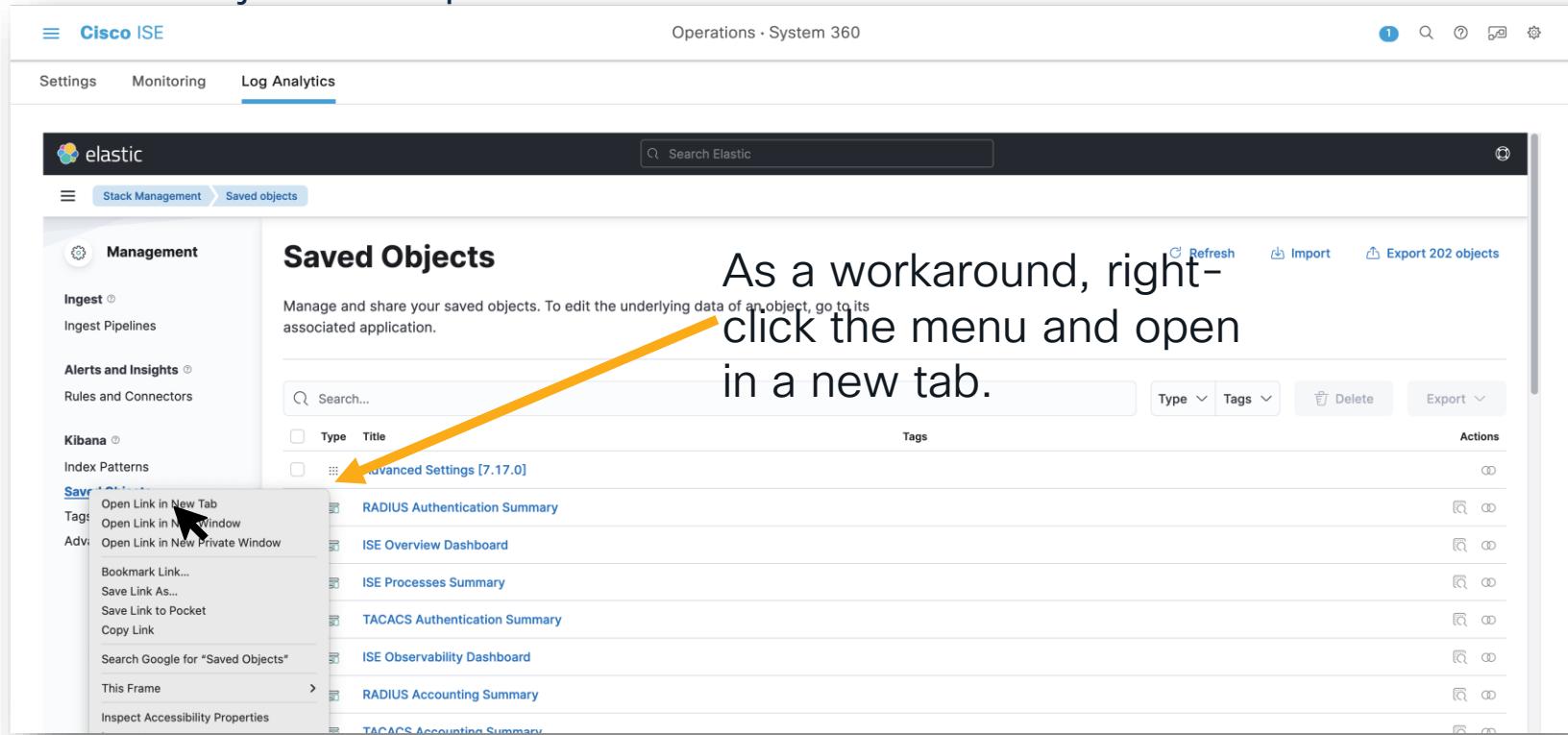
Delete Export

#CiscoLive BRKSEC-2897

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Log Analytics

Saved Objects – Export – Iframe Workaround



Operations - System 360

Cisco ISE

Settings Monitoring Log Analytics

elasticsearch

Search Elastic

Stack Management Saved objects

Management

Ingest

Alerts and Insights

Kibana

Saved objects

Tags

Advanced

Open Link in New Tab

Open Link in New Window

Open Link in New Private Window

Bookmark Link...

Save Link As...

Save Link to Pocket

Copy Link

Search Google for "Saved Objects"

This Frame

Inspect Accessibility Properties

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

Refresh Import Export 202 objects

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

Search...

Type Title

Tags

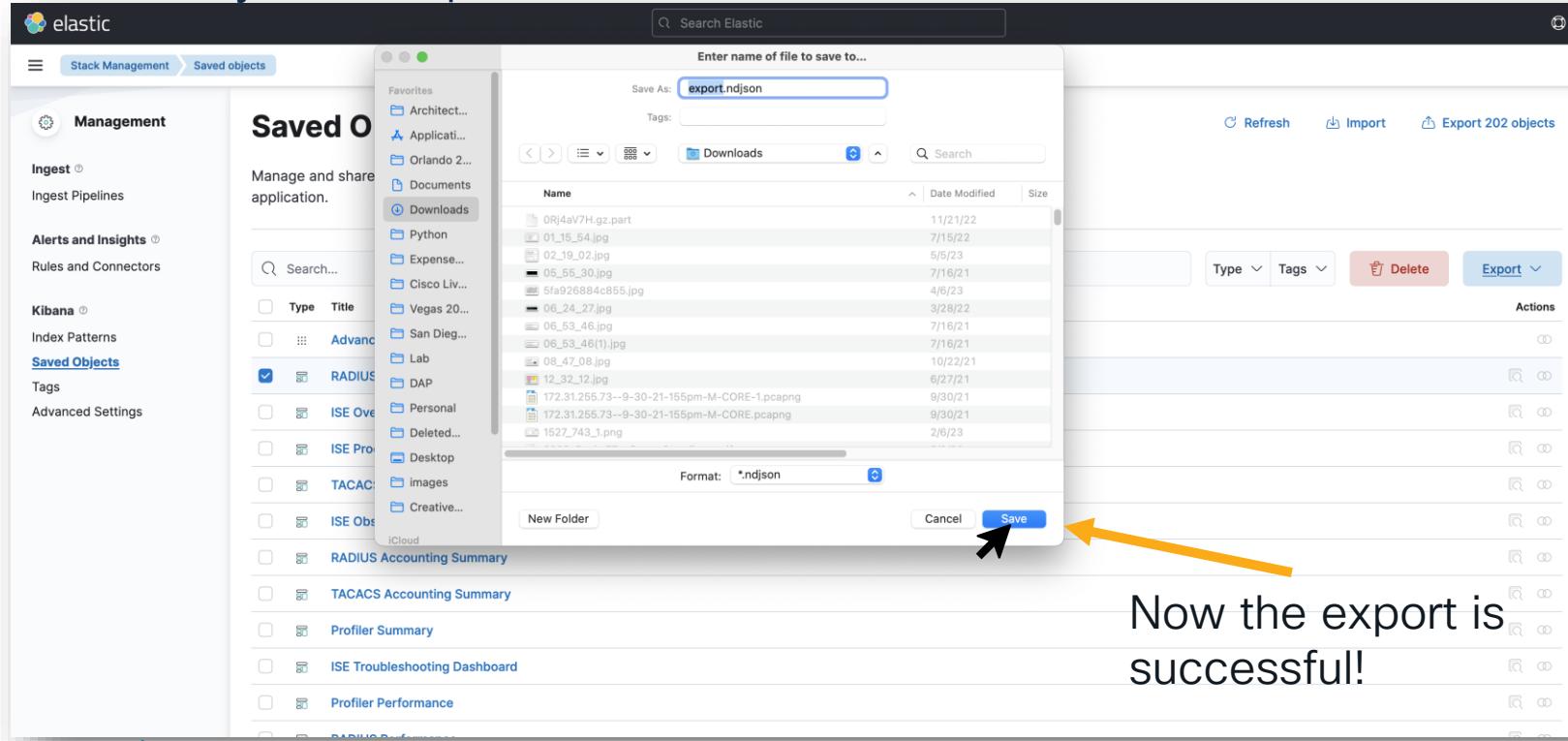
Delete Export

Actions

Refresh Import Export 202 objects

Log Analytics

Saved Objects - Export - Iframe Workaround



The screenshot shows the Elastic Stack Management interface with the 'Saved objects' tab selected. On the left, a sidebar lists various saved objects under 'Management', 'Ingest', 'Alerts and Insights', 'Kibana', and 'Saved Objects'. The 'Saved Objects' section is expanded, showing a list of items including 'RADIUS', 'ISE Overview', 'ISE Pro', 'TACACS', 'ISE Objects', 'RADIUS Accounting Summary', 'TACACS Accounting Summary', 'Profiler Summary', 'ISE Troubleshooting Dashboard', and 'Profiler Performance'. A modal window is open in the center, prompting the user to 'Enter name of file to save to...' with the input field containing 'export.ndjson'. Below this, a file browser shows a list of files in the 'Downloads' folder, including various image and log files. At the bottom of the modal are 'Cancel' and 'Save' buttons, with a large orange arrow pointing to the 'Save' button. The main interface on the right shows a list of 202 objects with columns for Type, Tags, and Actions, along with buttons for Refresh, Import, and Export.

Enter name of file to save to...

Save As: **export.ndjson**

Tags:

Name

Format: *.ndjson

Cancel **Save**

Refresh Import Export 202 objects

Now the export is successful!

Log Analytics

Saved Objects - Import

Cisco ISE Operations - System 360

Settings Monitoring Log Analytics

elastic Search Elastic

Stack Management Saved objects

Management Ingest Alerts and Insights Kibana

Saved Objects

Import objects into Kibana from ndjson files

Import Export 202 objects

Advanced Settings [7.17.0]

RADIUS Authentication Summary

ISE Overview Dashboard

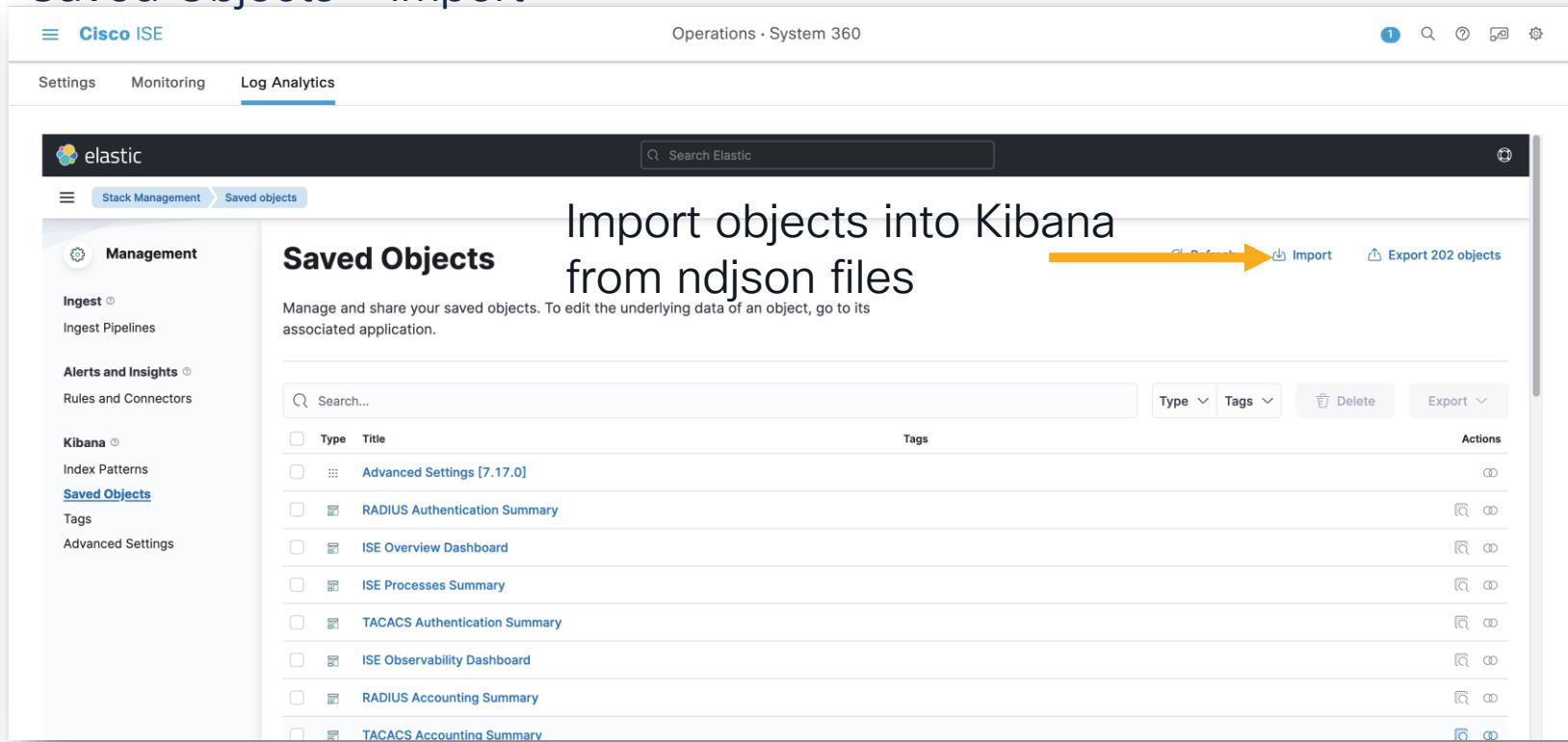
ISE Processes Summary

TACACS Authentication Summary

ISE Observability Dashboard

RADIUS Accounting Summary

TACACS Accounting Summary



Type	Title	Tags	Actions
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		∞

Log Analytics

Saved Objects - Import

Cisco ISE Operations - System 360

Settings Monitoring Log Analytics

elastic Stack Management Saved objects

Management Ingest Alerts and Insights Kibana

Saved Objects

Saved Objects

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

Search... Type Tags Actions

Type	Title	Tags	Actions
	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		

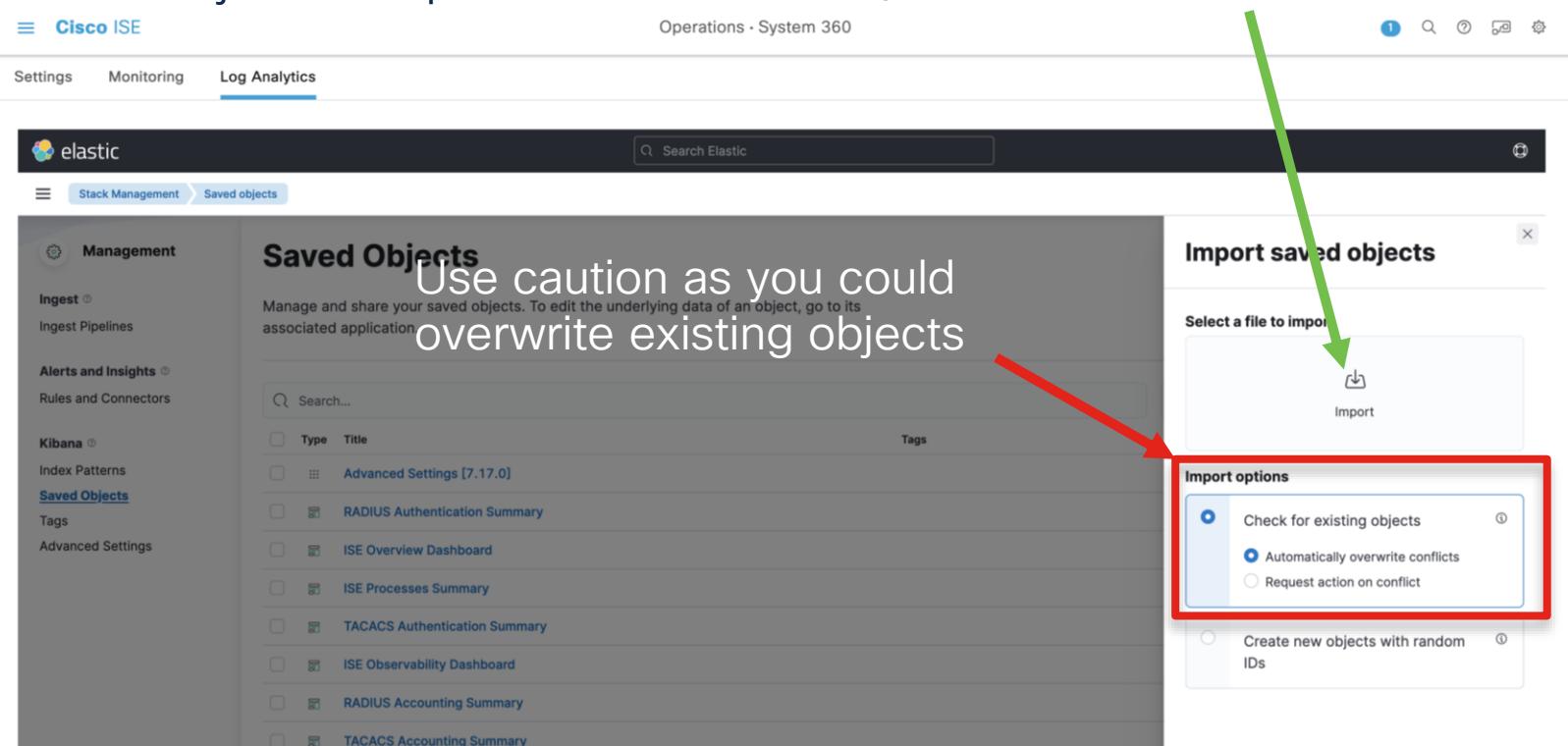
Refresh Import Export 202 objects



Log Analytics

Saved Objects - Import

Import file selection



The screenshot shows the Cisco ISE Log Analytics interface. The main page displays a list of saved objects under the 'Saved Objects' section. A prominent message at the top of this section reads: "Use caution as you could overwrite existing objects". To the right, a modal window titled "Import saved objects" is open, showing an "Import" button and an "Import options" section. The "Import options" section is highlighted with a red box and contains three radio buttons: "Check for existing objects" (selected), "Automatically overwrite conflicts", and "Request action on conflict". A green arrow points from the "Import" button in the modal to the "Import file selection" section at the top of the page. The top navigation bar includes tabs for "Settings", "Monitoring", and "Log Analytics", with "Log Analytics" being the active tab. The top right corner shows the "Operations - System 360" status and various system icons.

Log Analytics

Saved Objects - Import

The screenshot shows the Cisco ISE Log Analytics interface. The main title is 'Saved Objects - Import'. The left sidebar includes 'Management', 'Ingest', 'Alerts and Insights', 'Kibana', and 'Saved Objects' (which is selected). The main content area shows a 'Saved Objects' list with various items like 'Advanced Settings', 'RADIUS Authentication Summary', 'ISE Overview Dashboard', etc. A modal dialog titled 'Import saved objects' is open on the right. It has a 'Select a file to import' section with a file icon and 'Import' button, and an 'Import options' section. The 'Import options' section contains three radio buttons: 'Check for existing objects' (selected), 'Automatically overwrite conflicts', and 'Create new objects with random IDs'. The last option is highlighted with a red box and a red arrow pointing to it from the bottom left.

Using random IDs could lead to duplicate objects

Import saved objects

Select a file to import

Import

Import options

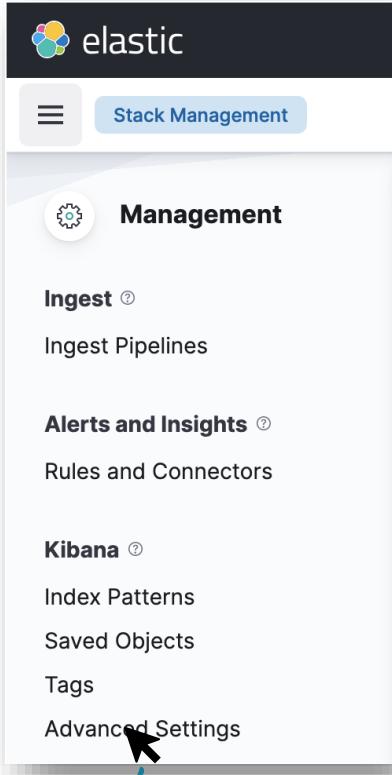
Check for existing objects

Automatically overwrite conflicts

Create new objects with random IDs

Log Analytics

Menu – Advanced Settings



The screenshot shows the 'Management' section of the Elastic Stack Management interface. The 'Advanced Settings' item is highlighted with a red arrow pointing to it. The interface includes a navigation bar with 'elastic' and 'Stack Management' buttons, and a sidebar with 'Management', 'Ingest', 'Alerts and Insights', 'Kibana', and 'Advanced Settings' sections.

- Management
- Ingest
- Alerts and Insights
- Kibana
- Advanced Settings

Log Analytics

Advanced Settings-Menu

The screenshot shows the Cisco ISE Log Analytics interface. The top navigation bar includes the Cisco ISE logo, the text "Operations · System 360", and an "Evaluation Mode 85 Days" indicator. The "Log Analytics" tab is selected in the main navigation bar. The main content area is the Kibana Settings page, which has a sidebar with "Management" sections for Ingest, Alerts and Insights, and Kibana, and a "Advanced Settings" section. The main content area has a "Settings" title and a "General" section. It includes configuration for "Disable Batch Compression" (radio button for "Off"), "Quote CSV values" (checkbox for "On" with a checked status), and "CSV separator" (input field containing a comma). A note in the General section cautions users about the risks of modifying advanced settings.

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

Operations · System 360

Evaluation Mode 85 Days

Settings Monitoring Log Analytics

elasticsearch

Stack Management Advanced Settings

Management

Ingest

Alerts and Insights

Kibana

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 align to an 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

Africa/Abidjan

Africa/Accra

Africa/Addis_Ababa

Africa/Algiers

Africa/Asmara

Africa/Asmera

Africa/Bamako

Africa/Bangui

Africa/Banjul

Africa/Bissau

Africa/Blantyre

Africa/Brazzaville

Africa/Bujumbura

Africa/Cairo

Africa/Casablanca

Africa/Ceuta

Africa/Conakry

Africa/Dakar

Africa/Dar_es_Salaam

Browser

dateNanosFormat

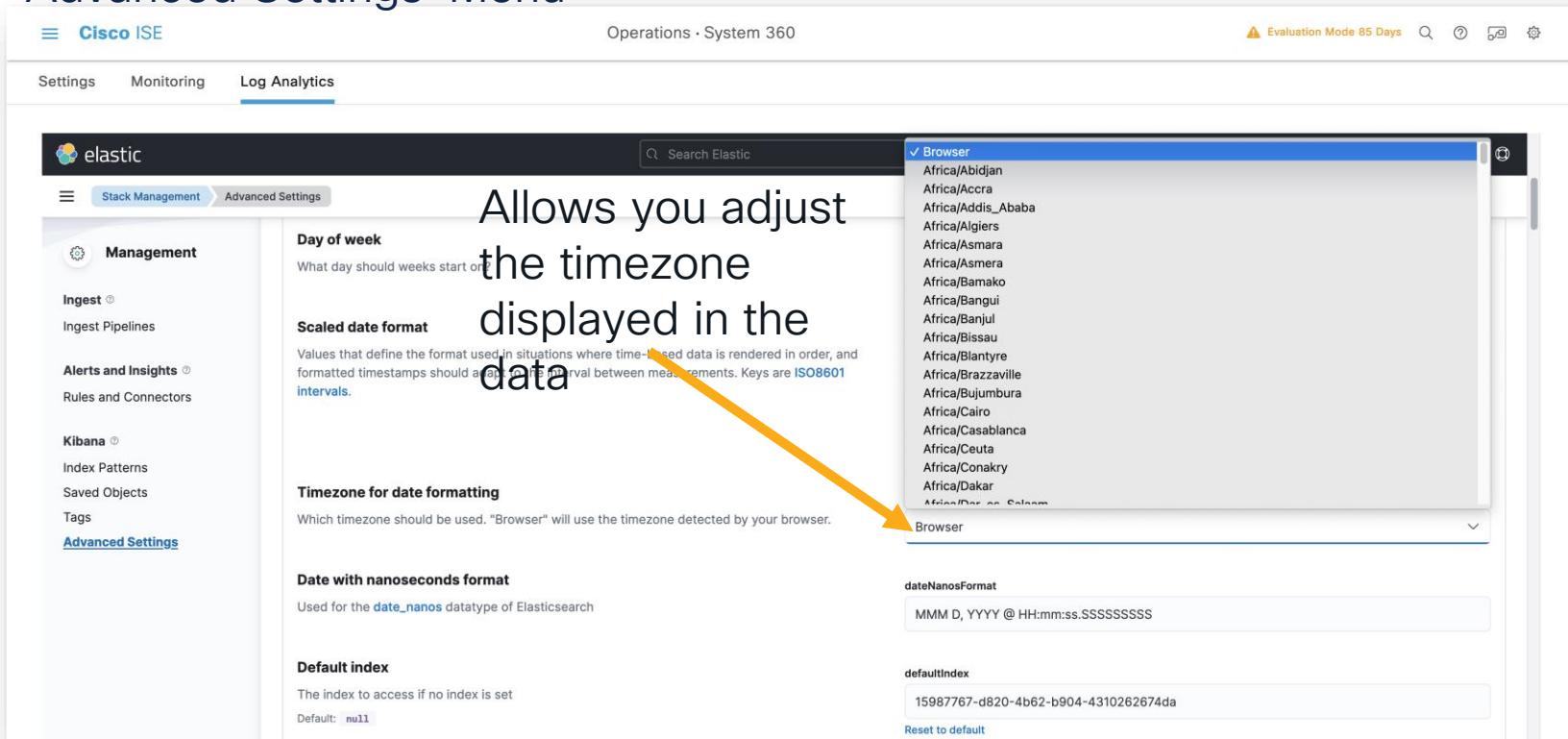
MMM D, YYYY @ HH:mm:ss.SSSSSSSS

defaultIndex

15987767-d820-4b62-b904-4310262674da

Reset to default

Allows you adjust the timezone displayed in the data



Log Analytics

Advanced Settings-Menu

Operations · System 360

Cisco ISE

Log Analytics

elastic

Search Elastic

Stack Management Advanced Settings

Management

Ingest

Alerts and Insights

Kibana

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",`

Evaluation Mode 85 Days

Toggle dark mode

Log Analytics

Advanced Settings-Menu

The screenshot shows the 'Advanced Settings' section of the Kibana configuration interface. On the left, a sidebar lists management, ingest, alerts, Kibana, and advanced settings. The main area contains several configuration items with a large orange arrow pointing from the 'Dark mode' section to the 'Save changes' button at the bottom right.

- shorten fields**: Shorten long fields, for example, instead of foo.bar.baz, show f.b.baz. Configuration: `shortDots:enable` (radio button off, checked), `sort:options` (JSON: `{"unmapped_type": "boolean"}`).
- 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 counteract this we are testing if storing parts of the URL in session storage could help. Please let us know how it goes! Configuration: `state:storeInSessionStorage` (radio button off, checked), `theme:darkMode` (checkbox checked, value 'On'), `theme:version` (dropdown 'v8').
- 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). Configuration: `timepicker:quickRanges` (JSON array with two objects):
 - { "from": "now/d", "to": "now/d", "display": "Today" }
 - { "from": "now/w", "to": "now/w", "display": "This week" }

Don't forget to save!

At the bottom, a message says '1 unsaved setting' and features 'Cancel changes' and 'Save changes' buttons. An orange arrow points from the 'Dark mode' section to the 'Save changes' button.

Demo

Thank You!

cisco *Live!*

Let's go

#CiscoLive