
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.

Cisco live!

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

The bridge to possible

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

Cisco Log Analysis & Remediation Kiosk

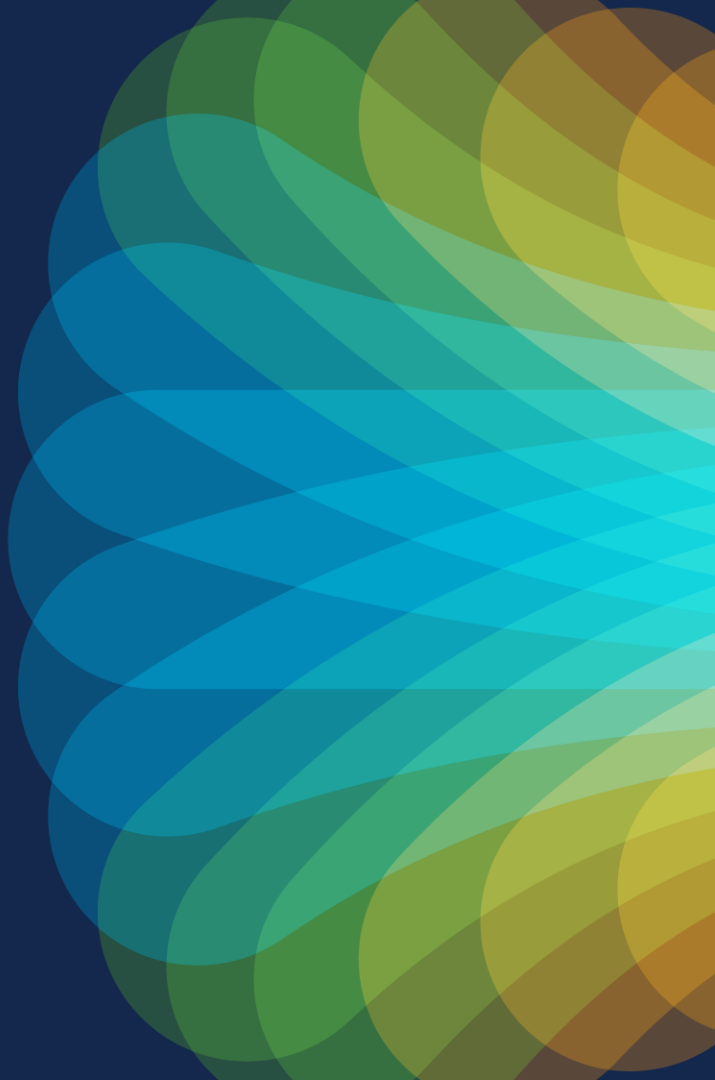
Clark Gambrel – Principal Engineer
@clarkgambrel

BRKSEC-2897

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

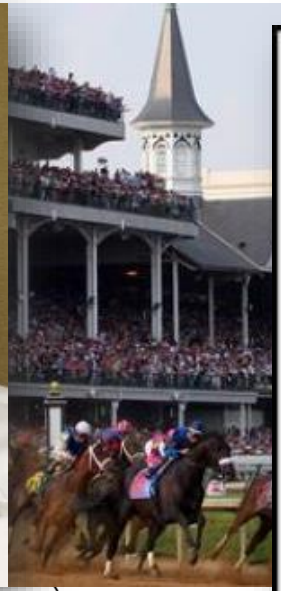
@ClarkGambrel

Clark Gambrel, CCIE #18179

Principal Engineer

cgambrel@cisco.com

@ClarkGambrel



KENTUCKY

"I might be a redneck"

Kentucky is known for…

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

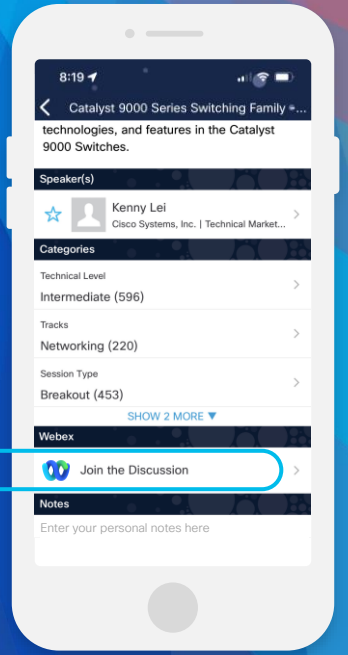
Questions?

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

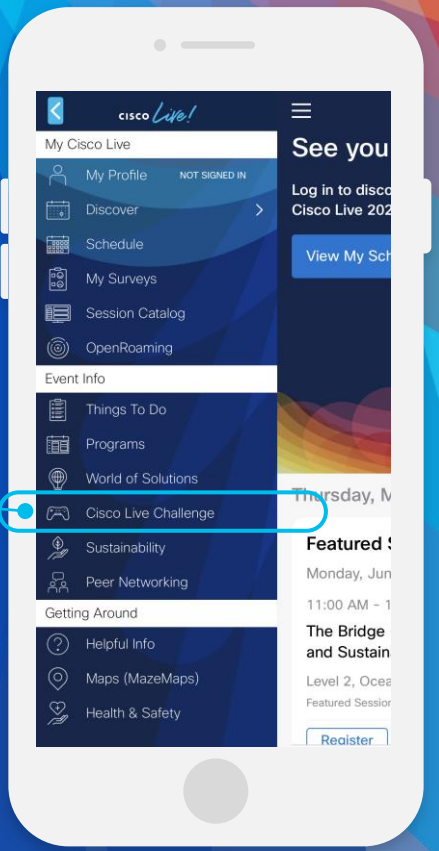
Cisco Live
Challenge

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:

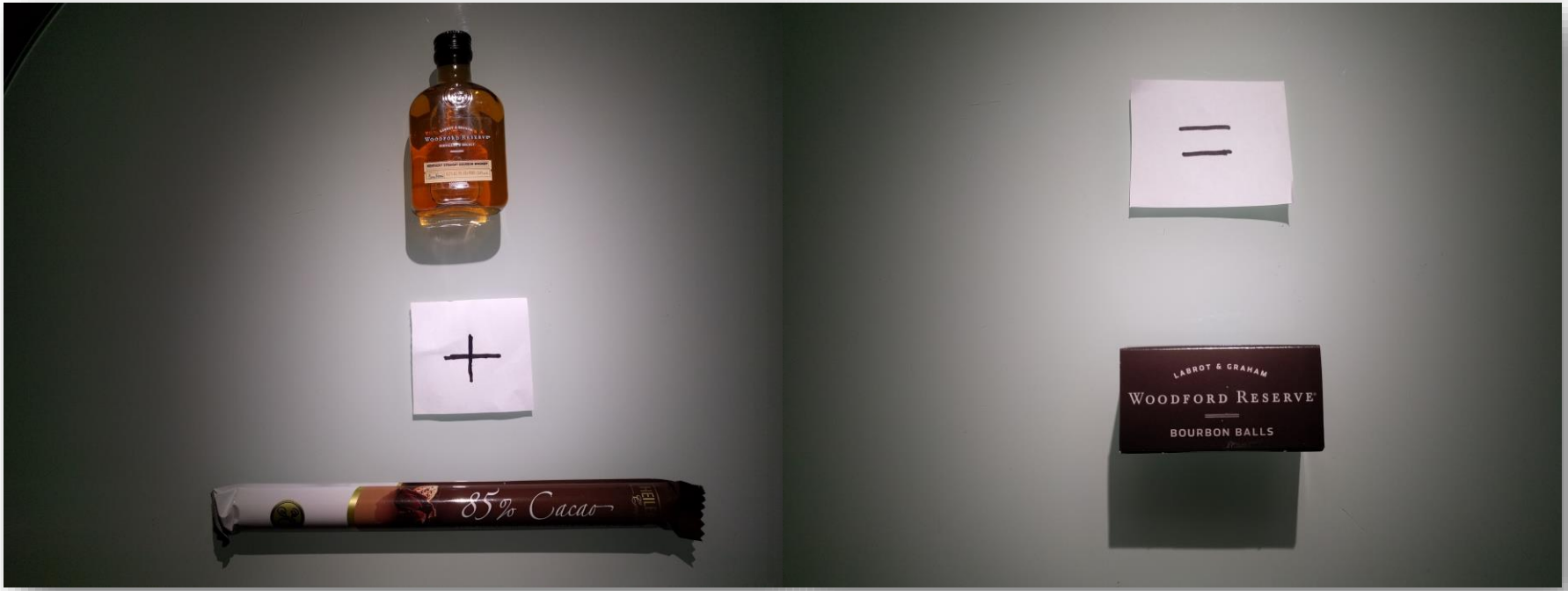


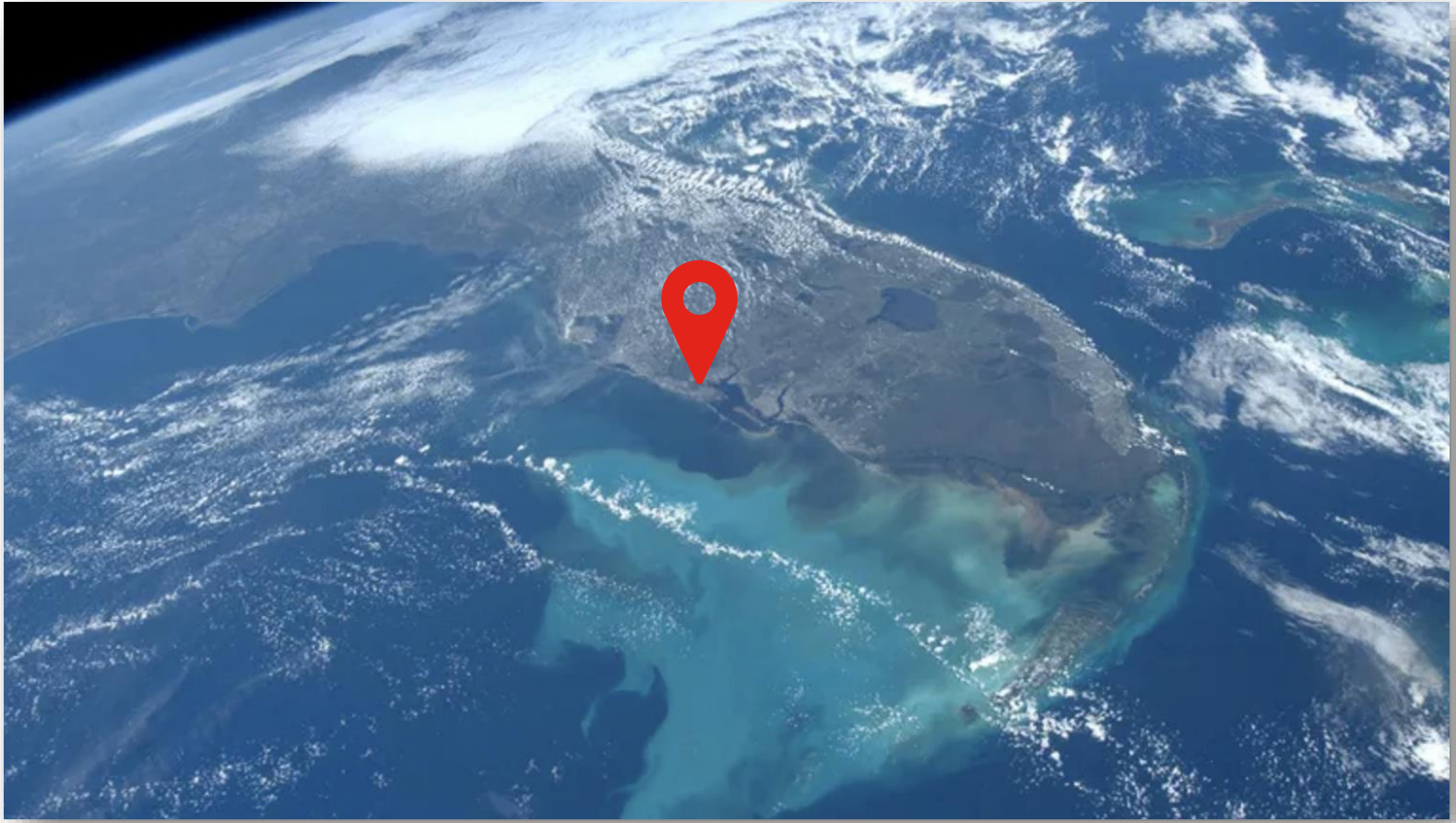
Continue your education

- 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

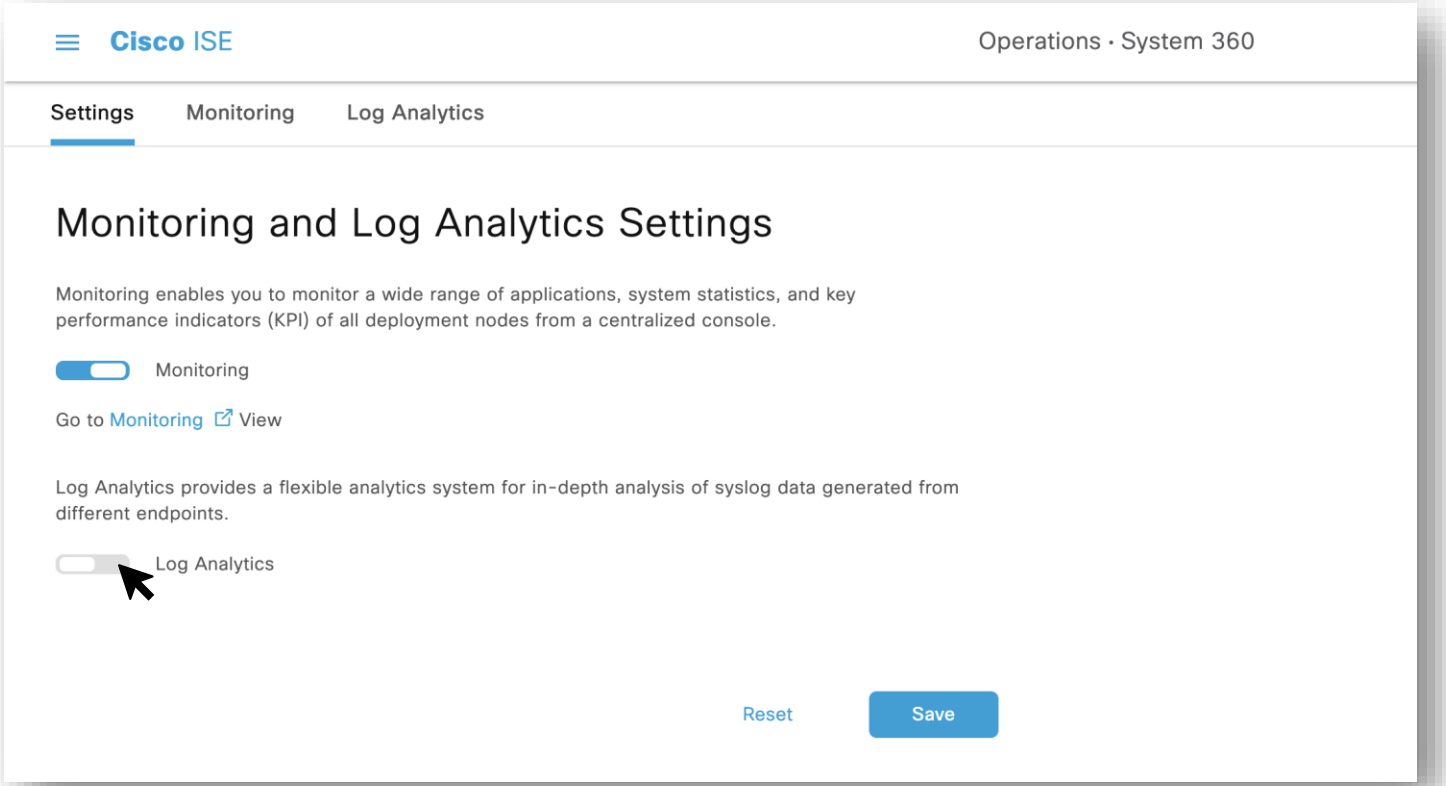
Log Analytics

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

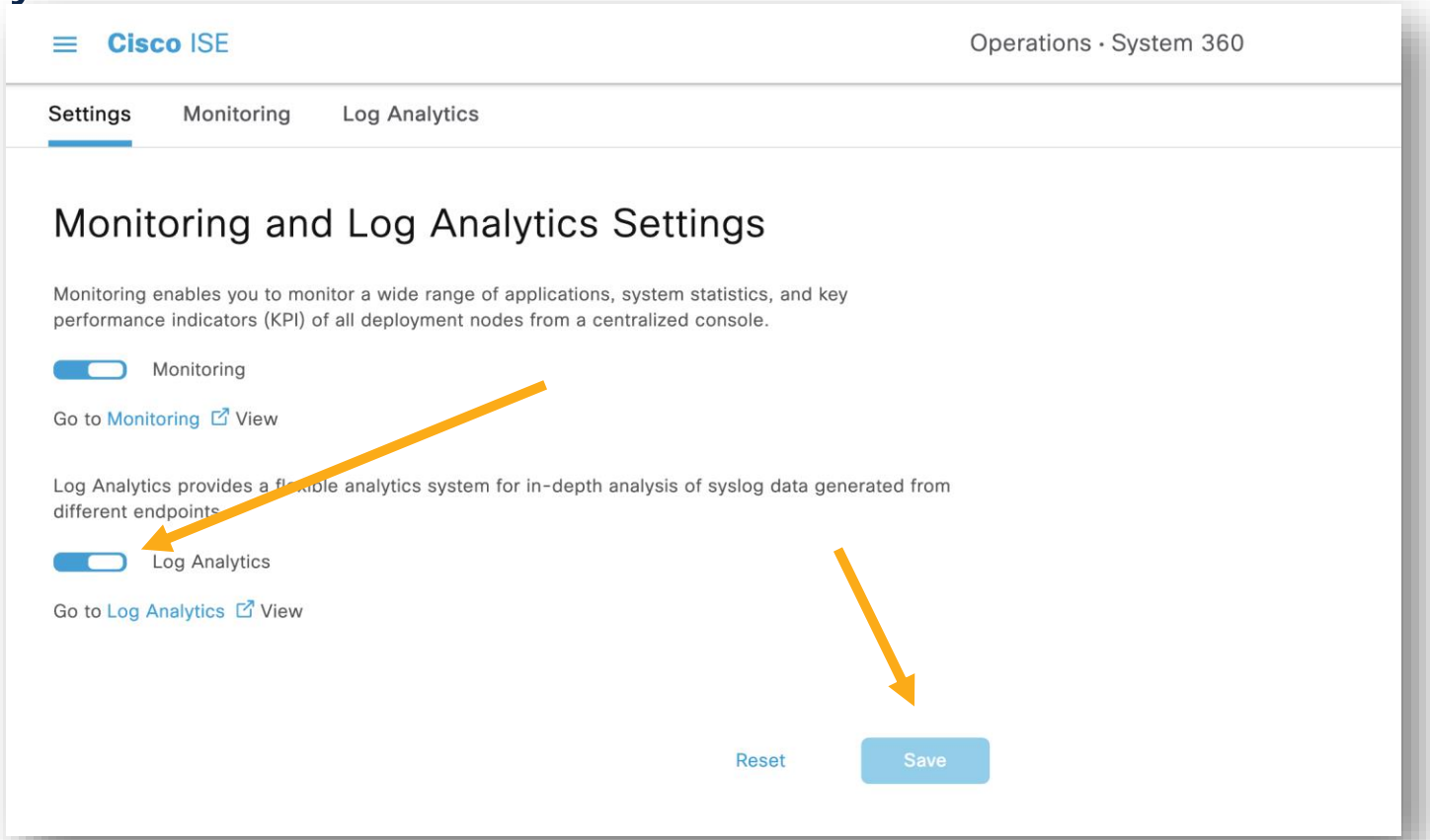
Log Analytics

Overview



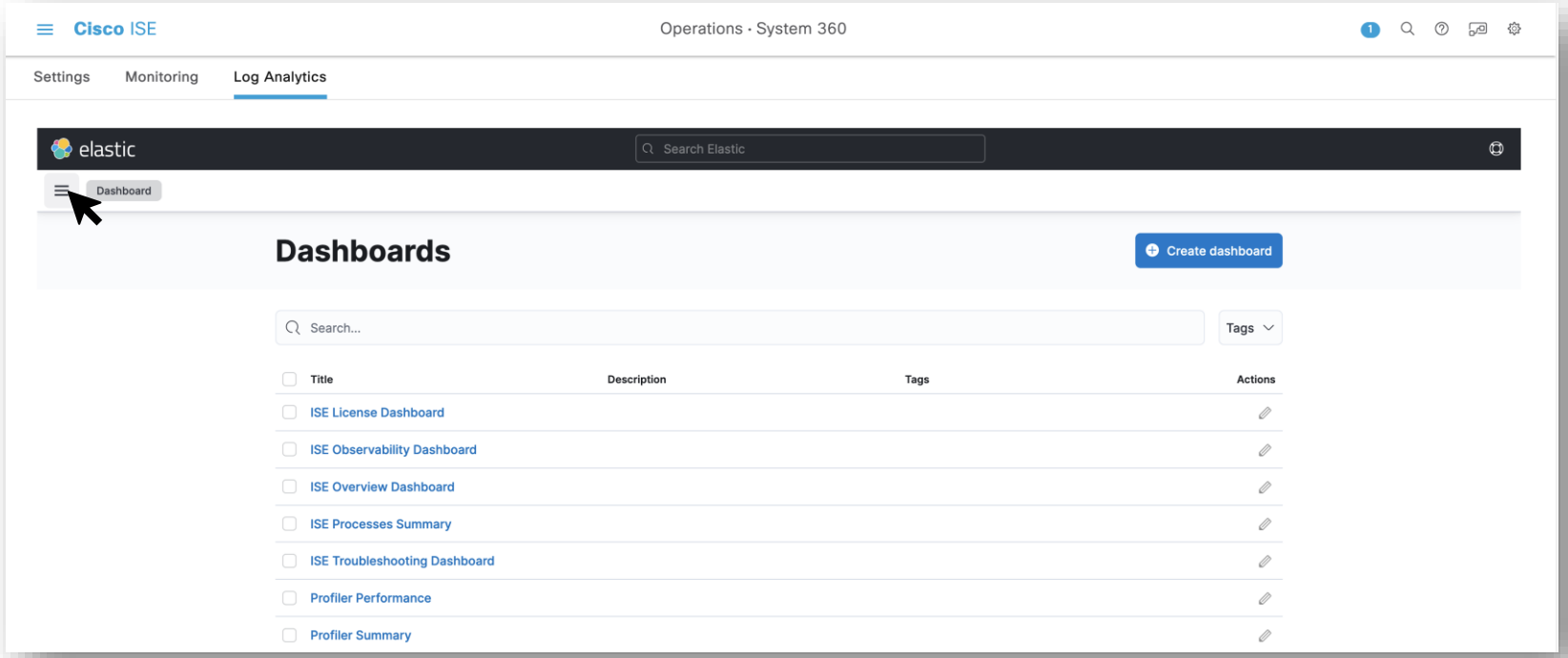
Log Analytics

Enabling



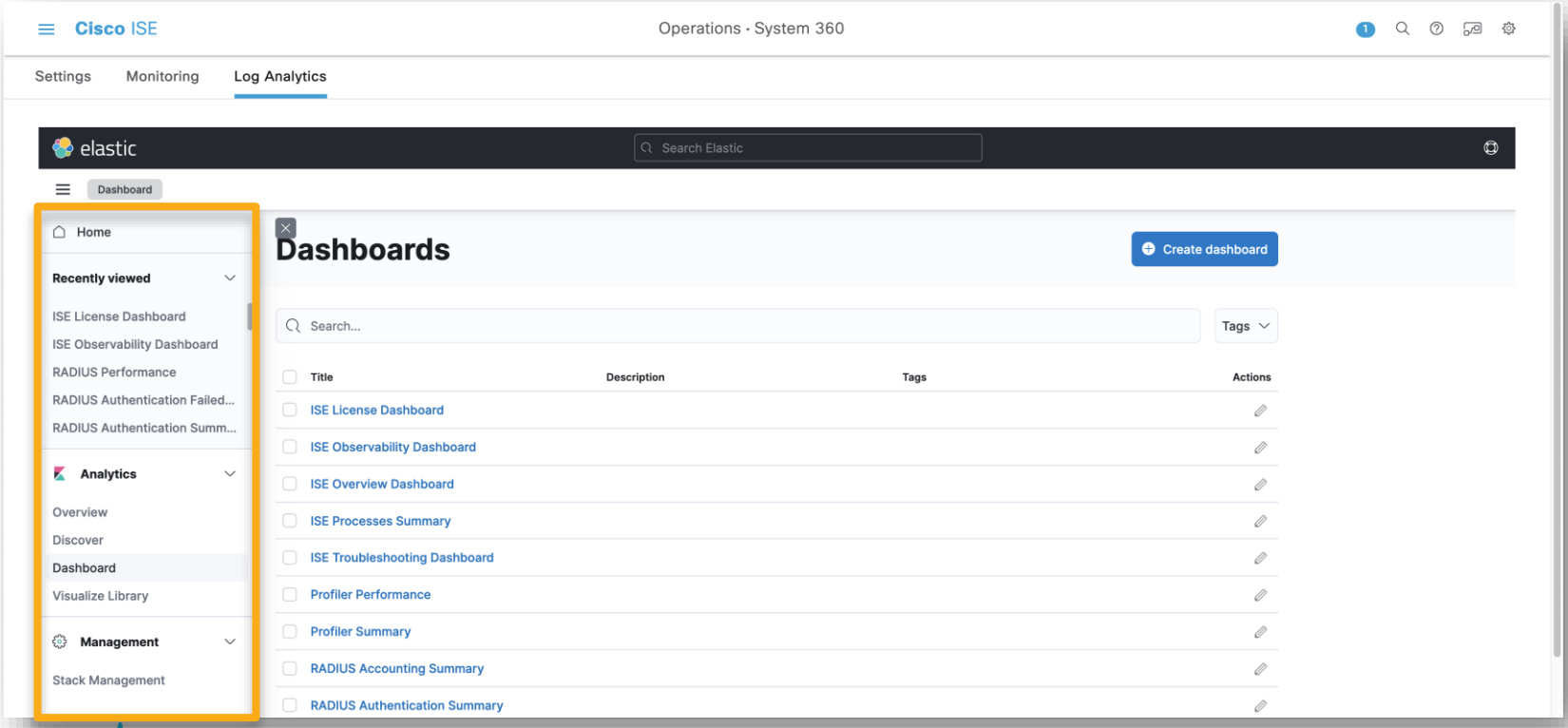
Log Analytics

Dashboards



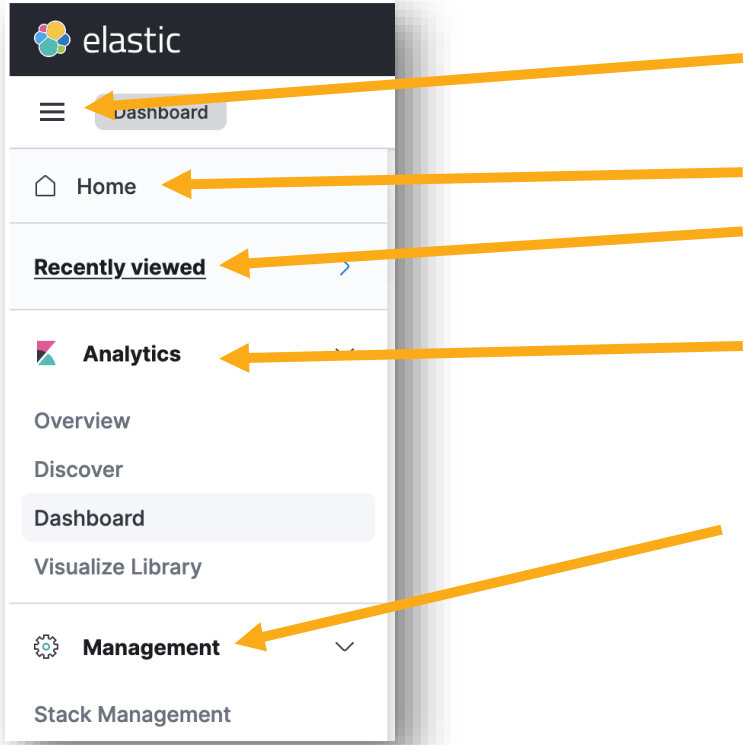
Log Analytics

Navigation



Log Analytics

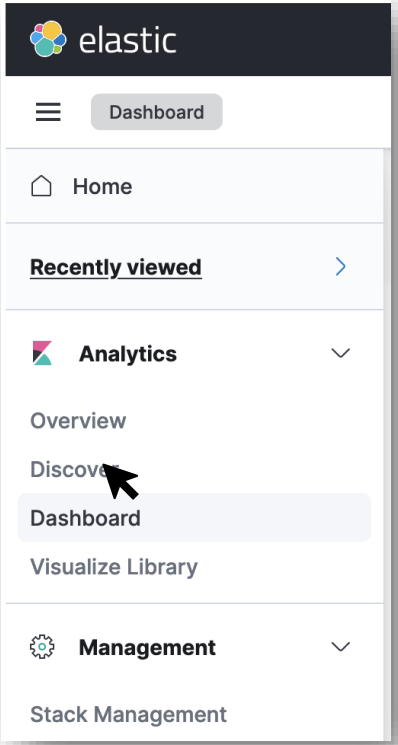
Navigation – Menus



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

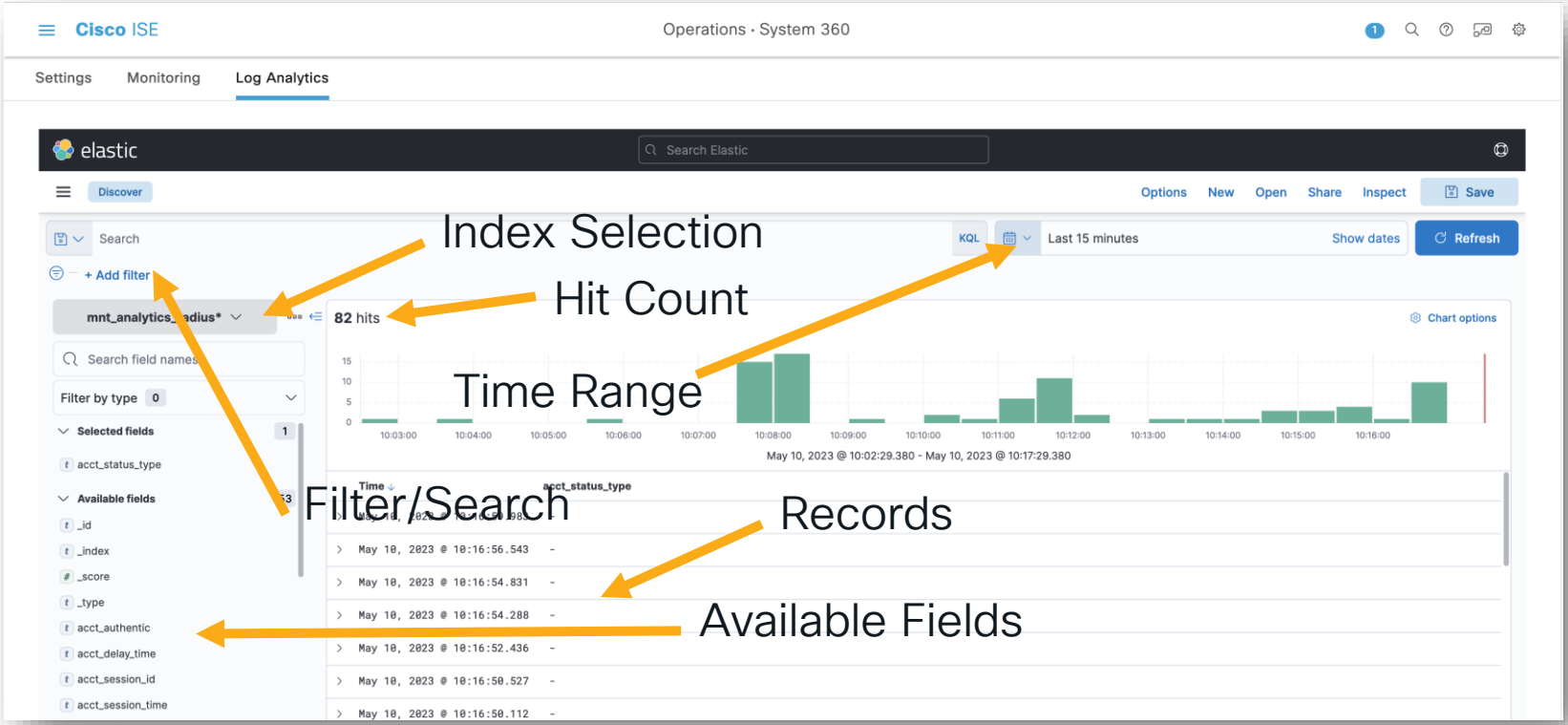
Log Analytics

Navigation – Menus



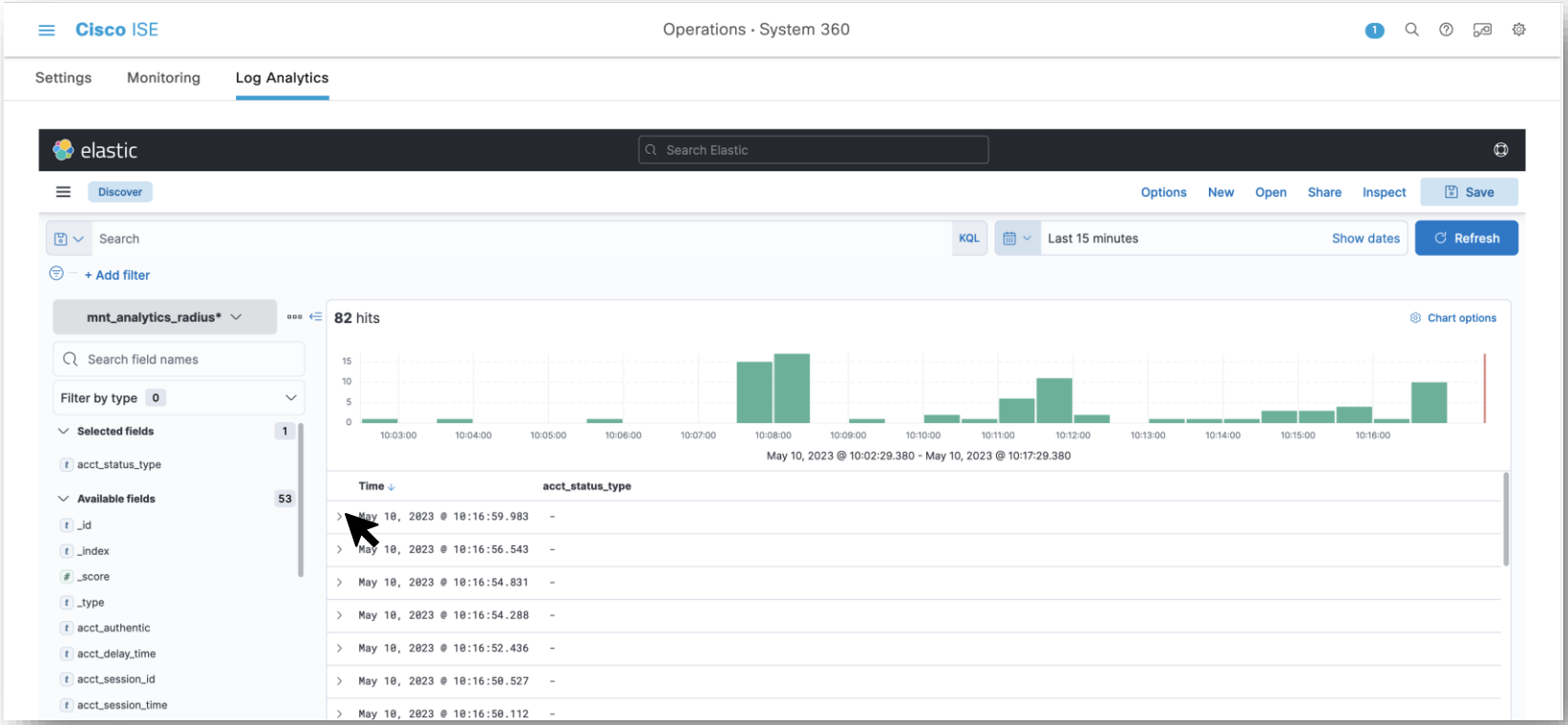
Log Analytics

Menu – Discover



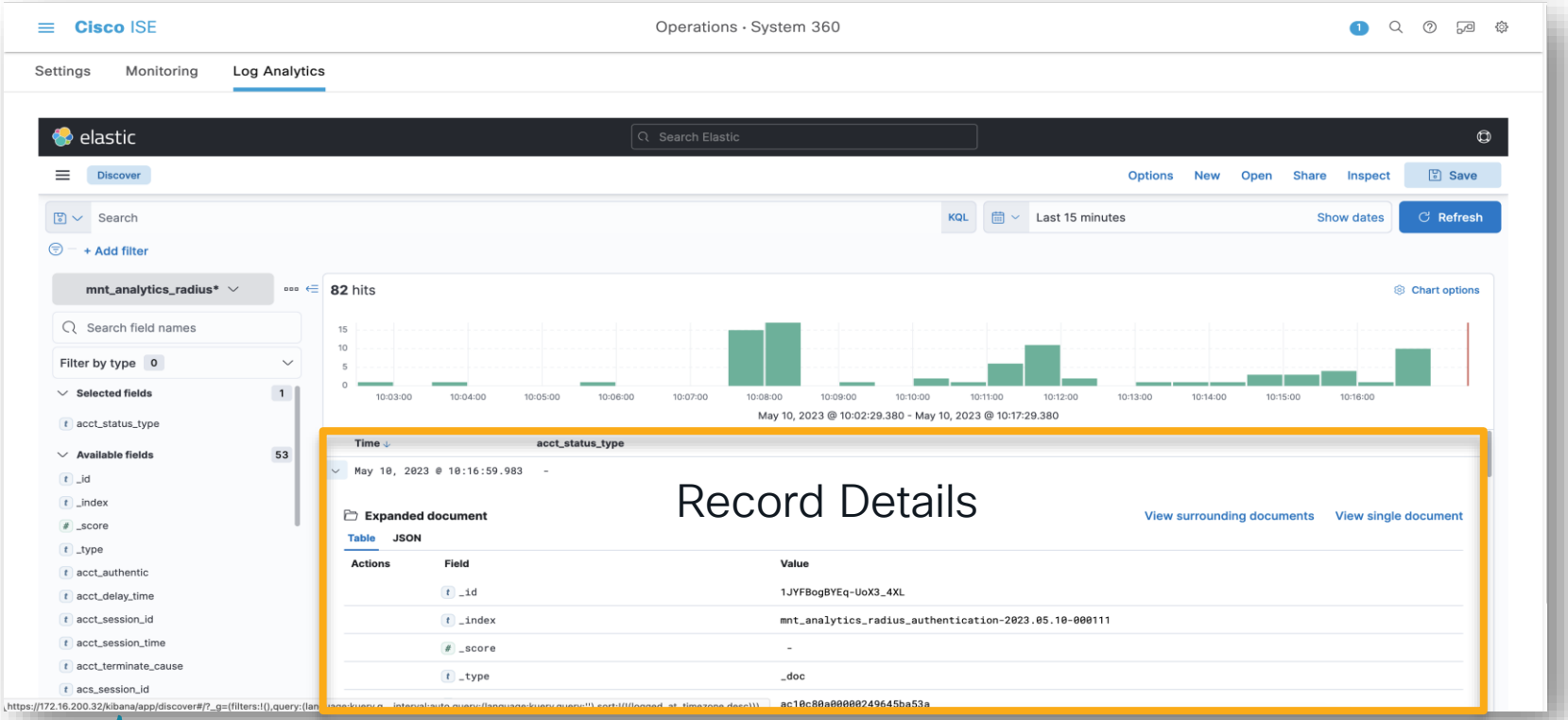
Log Analytics

Menu – Discover



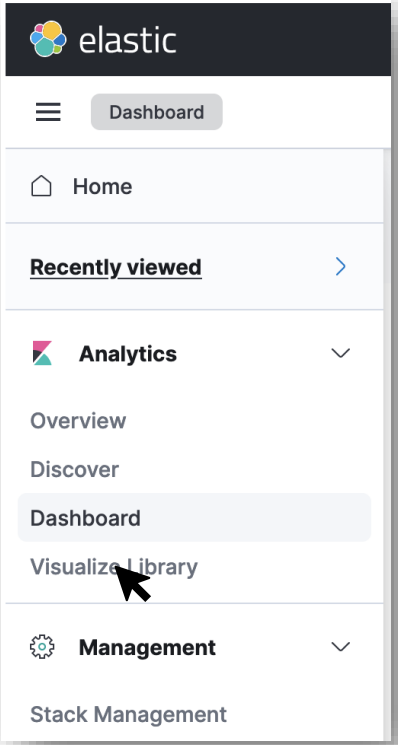
Log Analytics

Menu - Discover



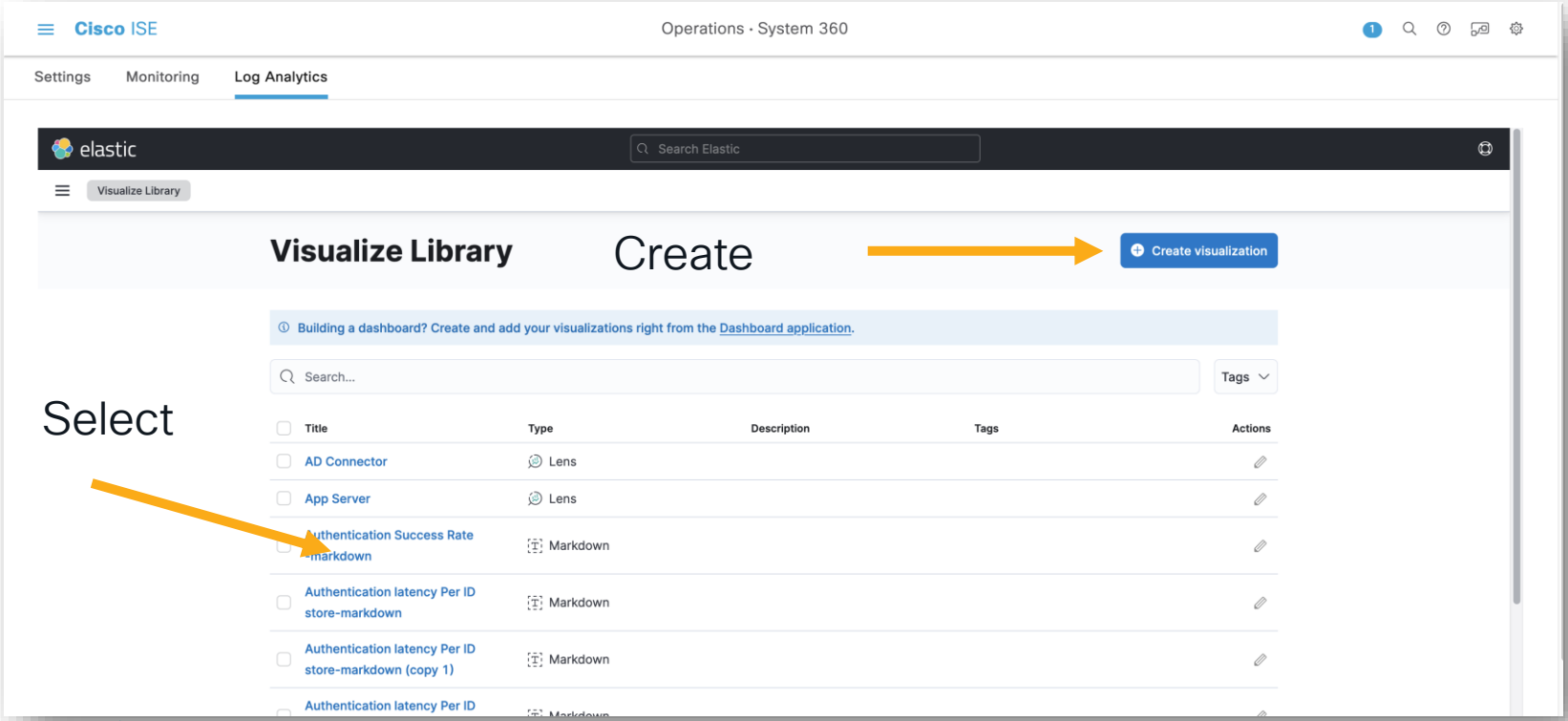
Log Analytics

Navigation – Menus



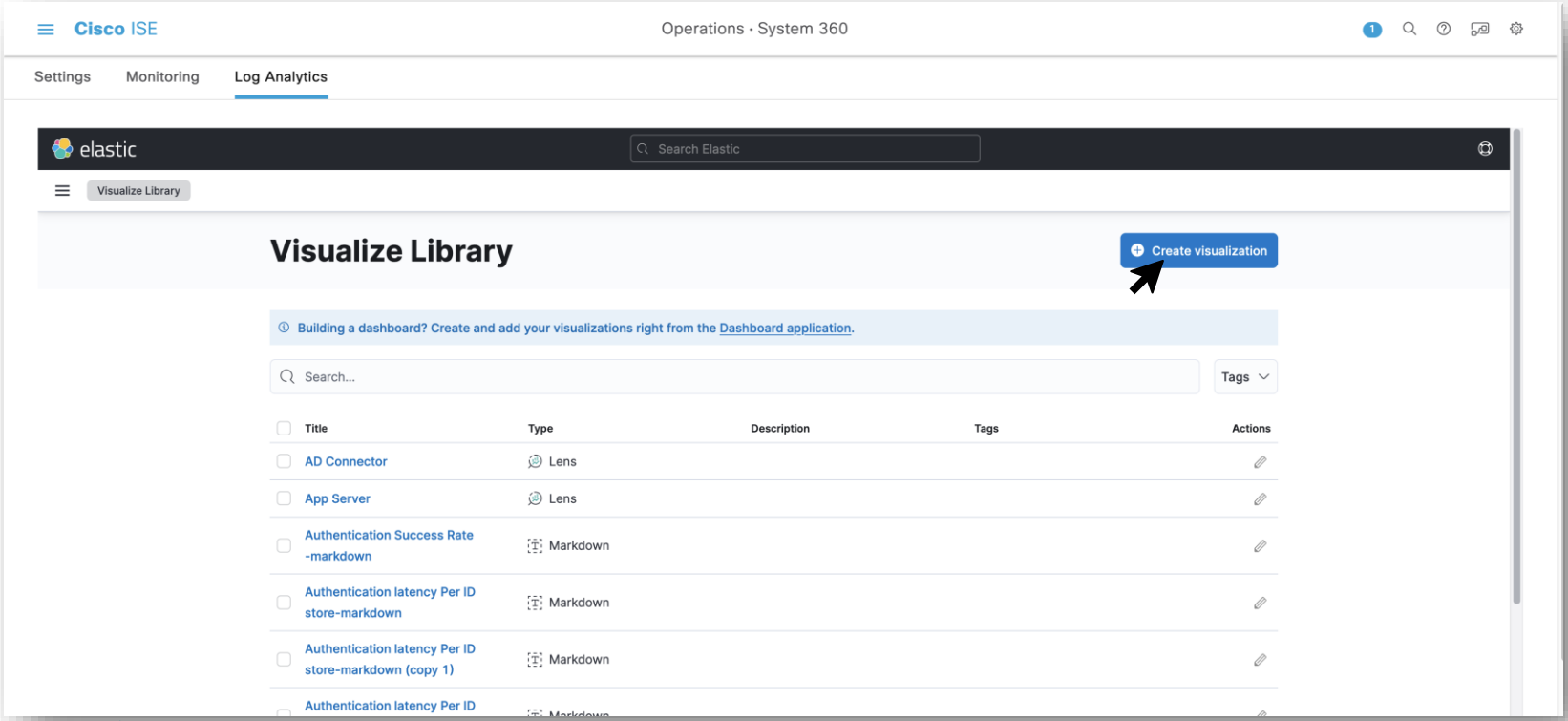
Log Analytics

Menu – Visualizations



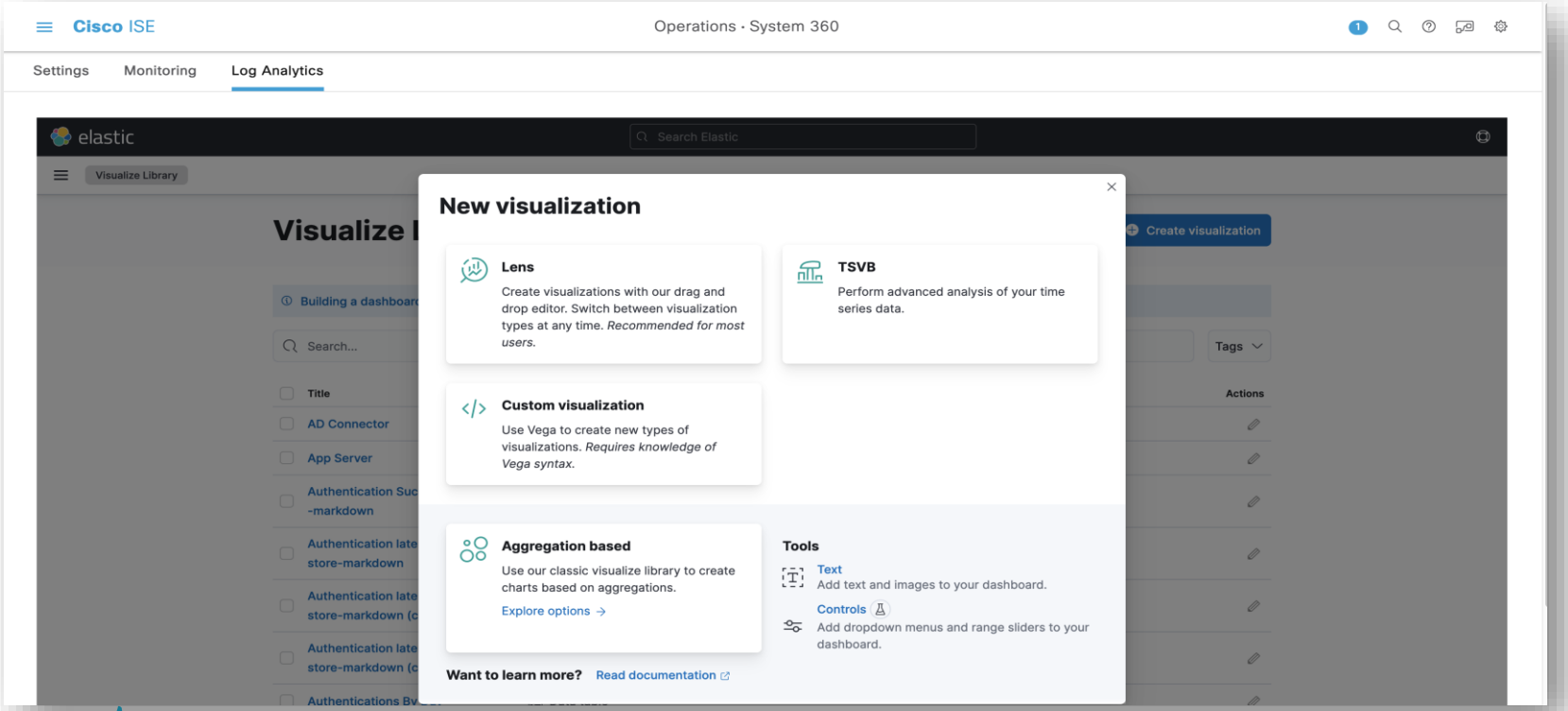
Log Analytics

Visualizations - Create



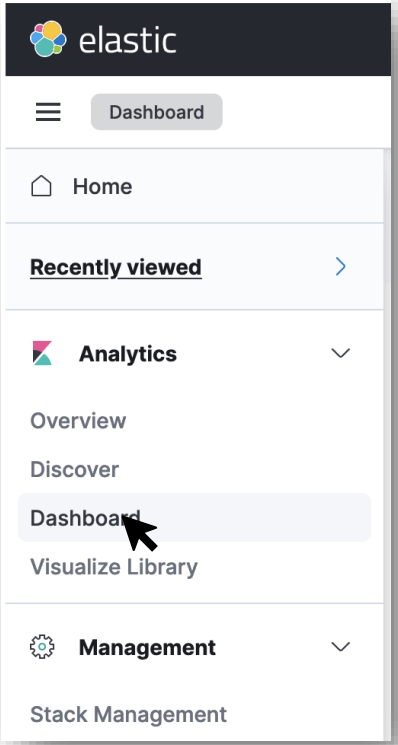
Log Analytics

Visualizations - Create



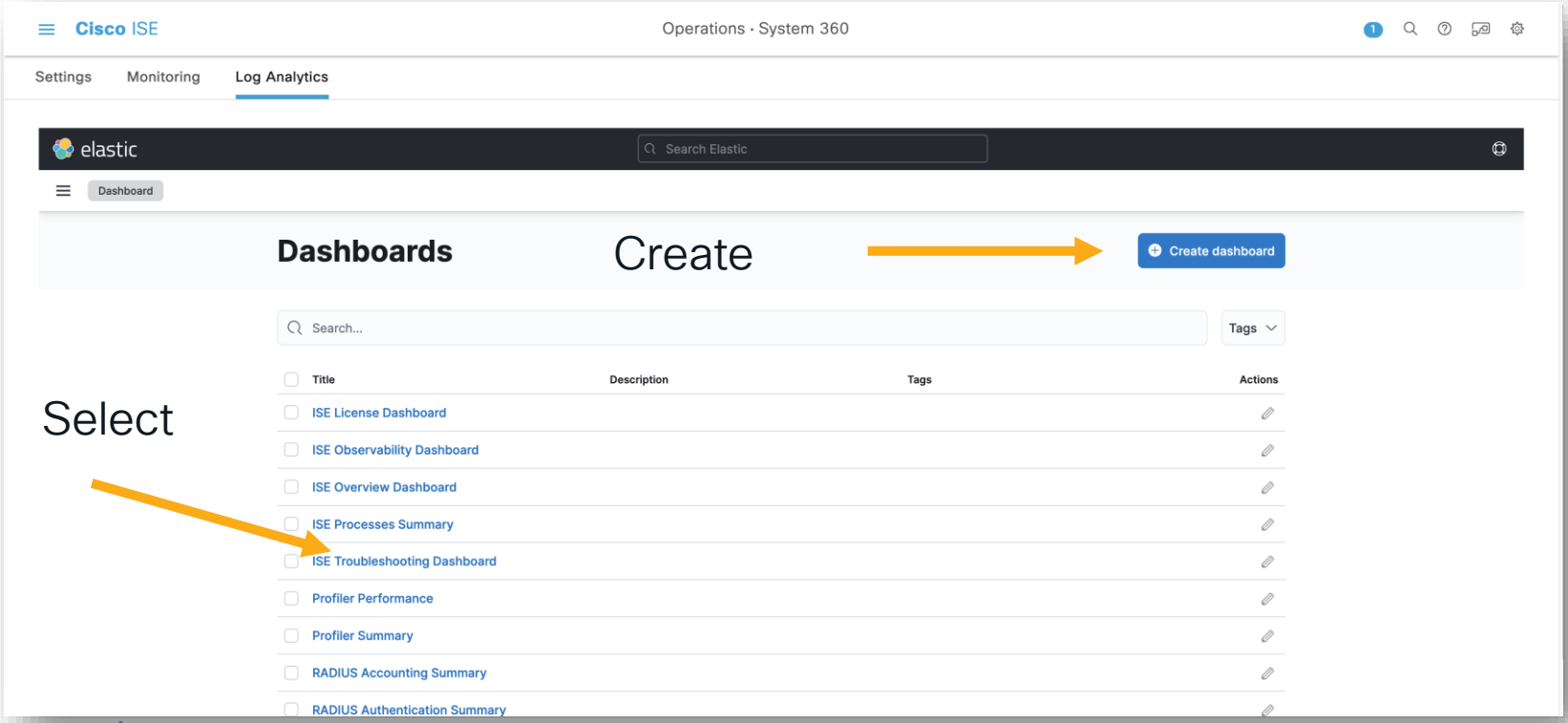
Log Analytics

Navigation – Menus



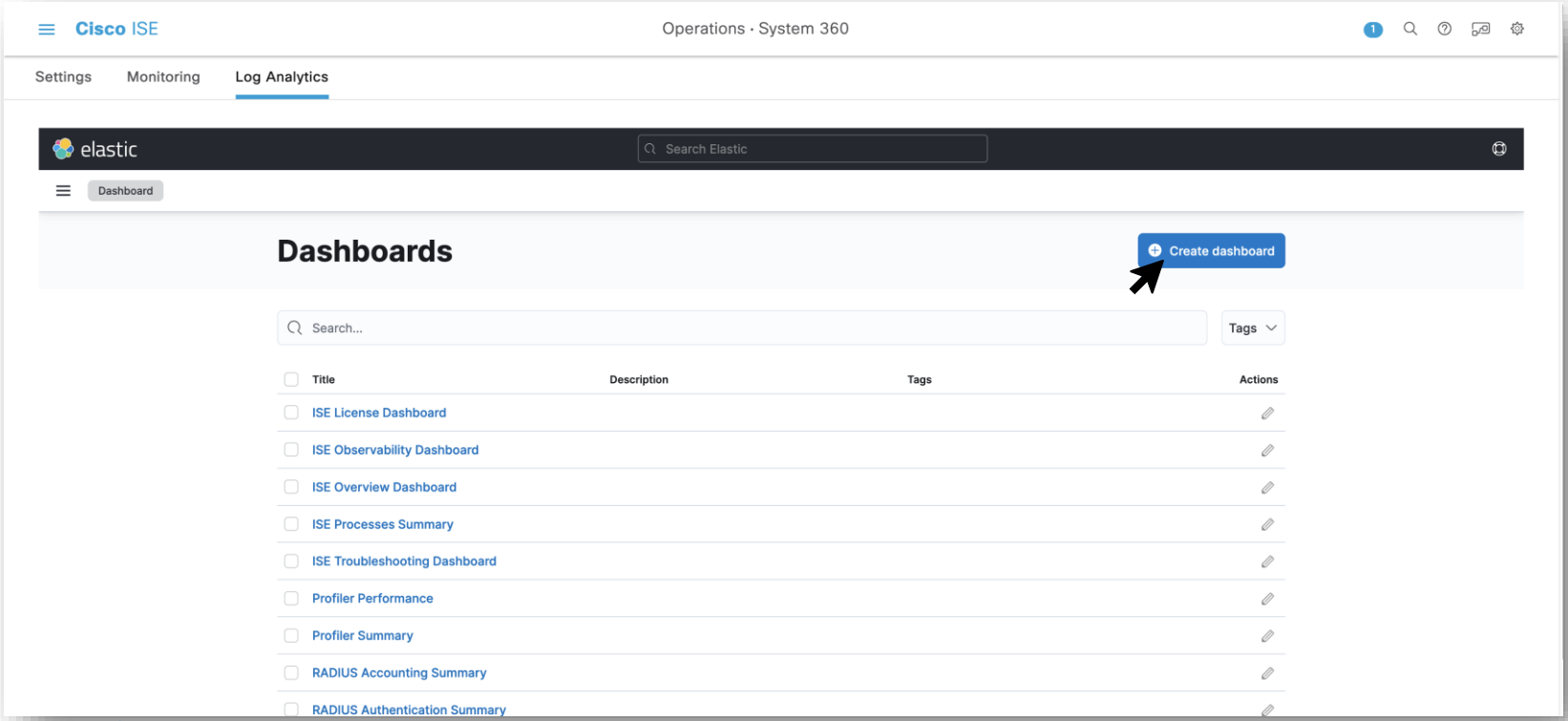
Log Analytics

Menu – Dashboards



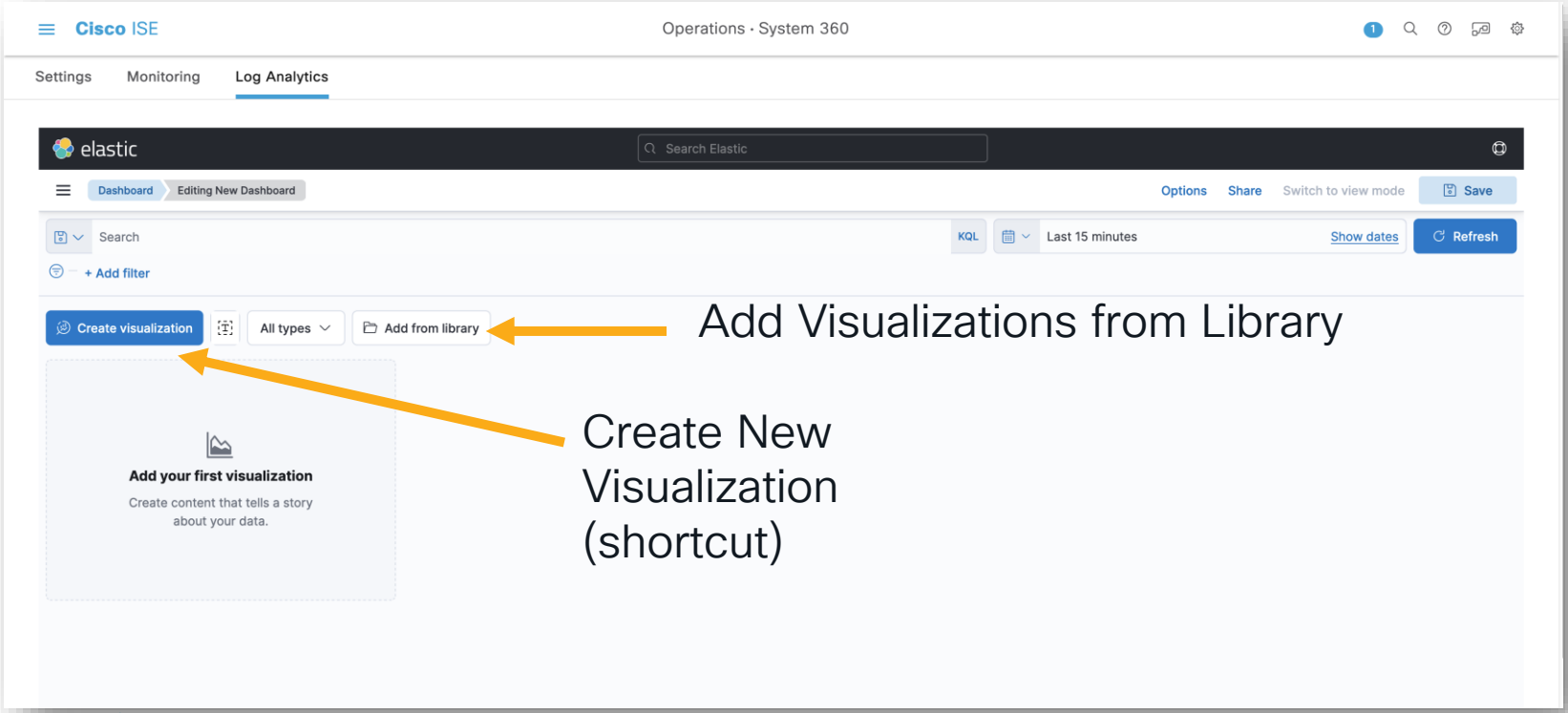
Log Analytics

Dashboards - Create



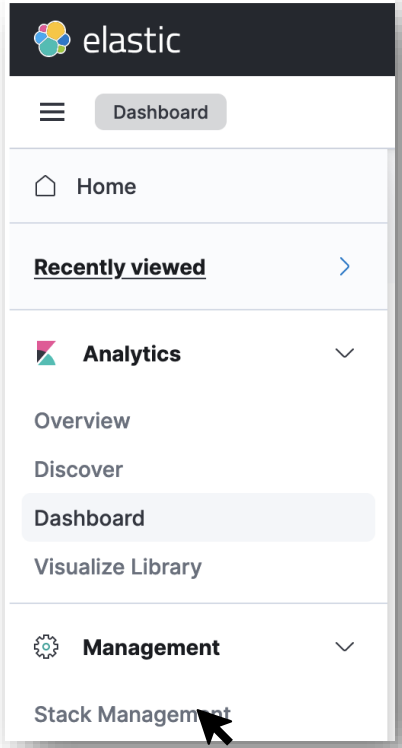
Log Analytics

Dashboards - Create



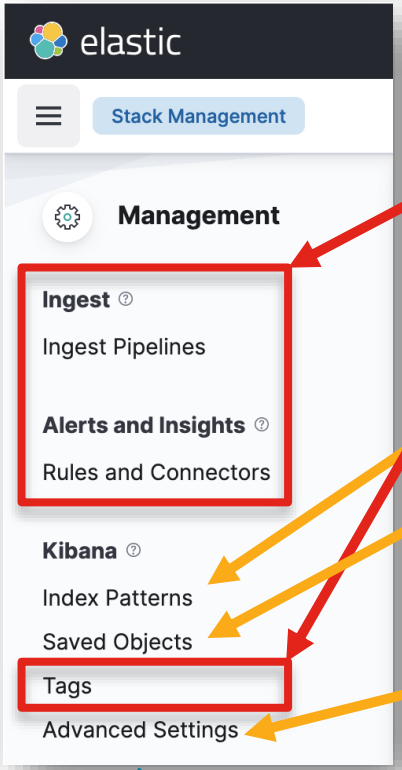
Log Analytics

Navigation – Menus



Log Analytics

Menus – Stack Management



Not currently supported

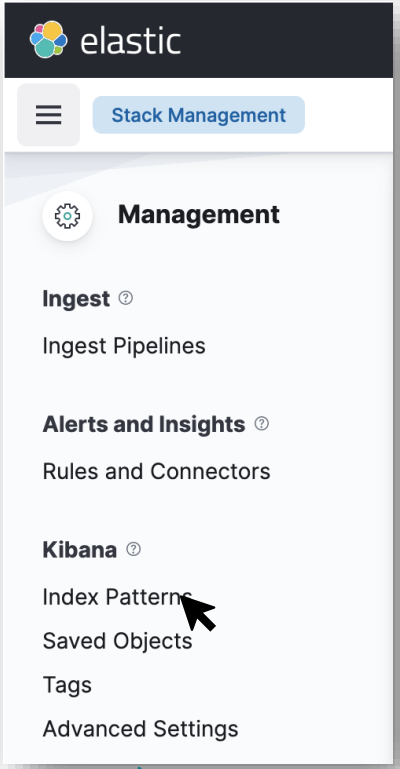
Kibana index search patterns

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

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

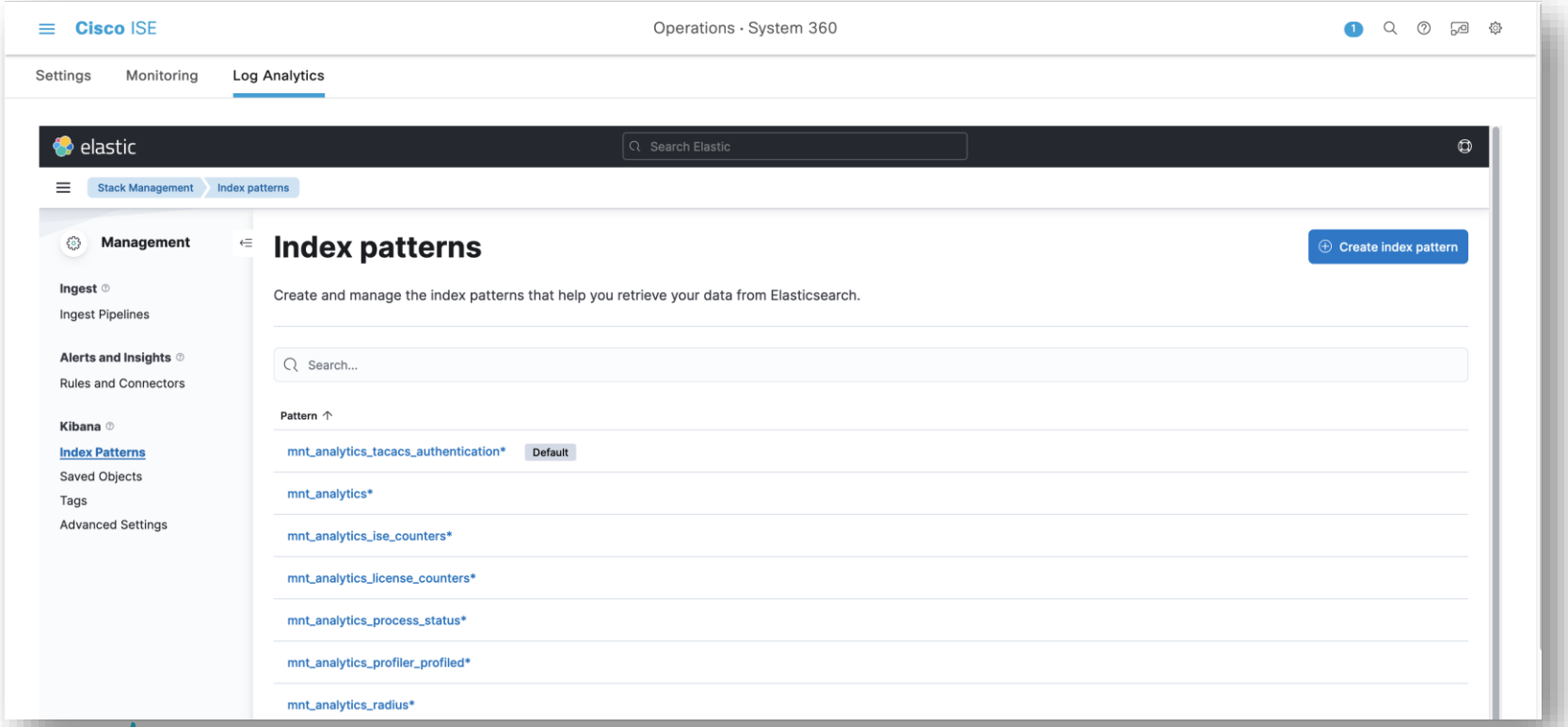
Log Analytics

Menu - Index Patterns



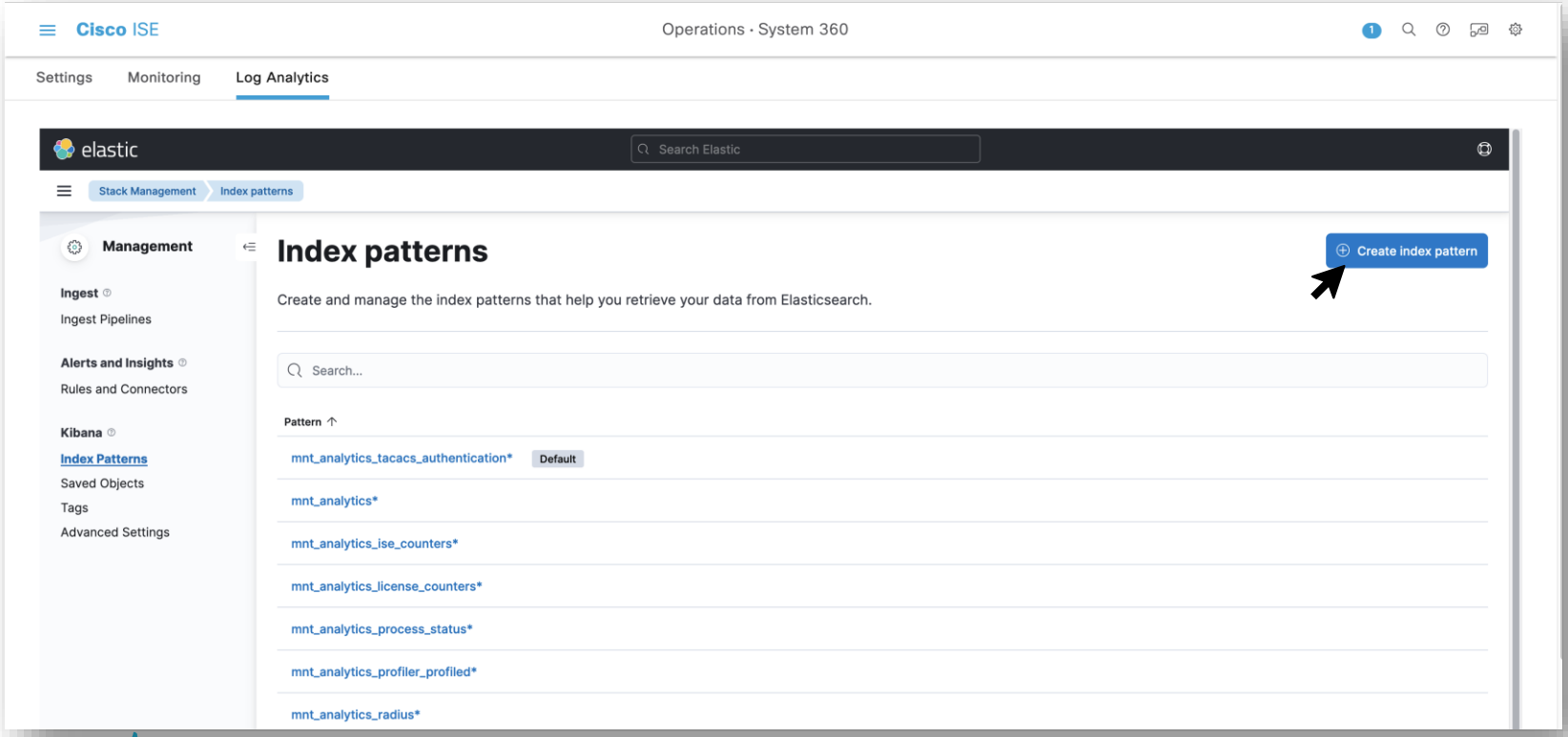
Log Analytics

Menu – Index Patterns



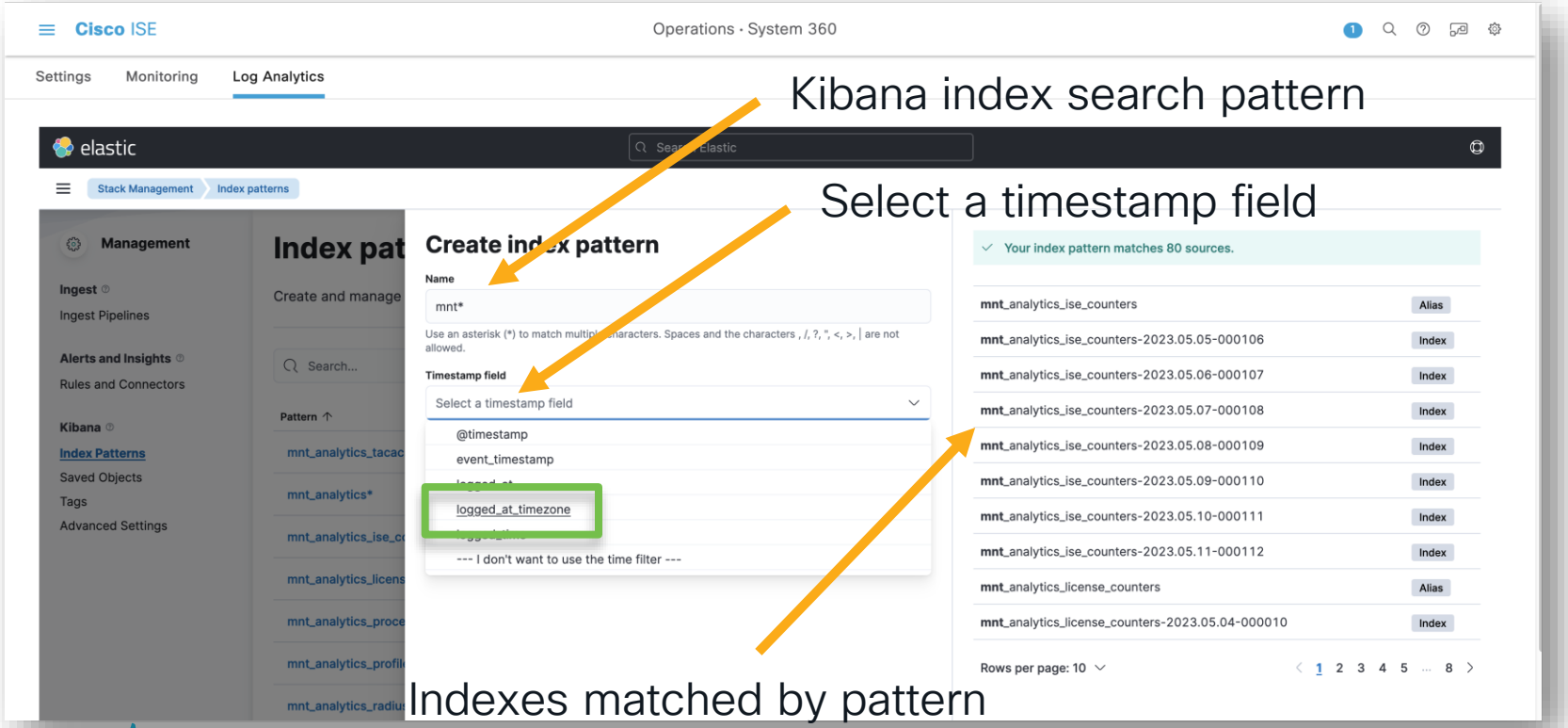
Log Analytics

Index Patterns - Create



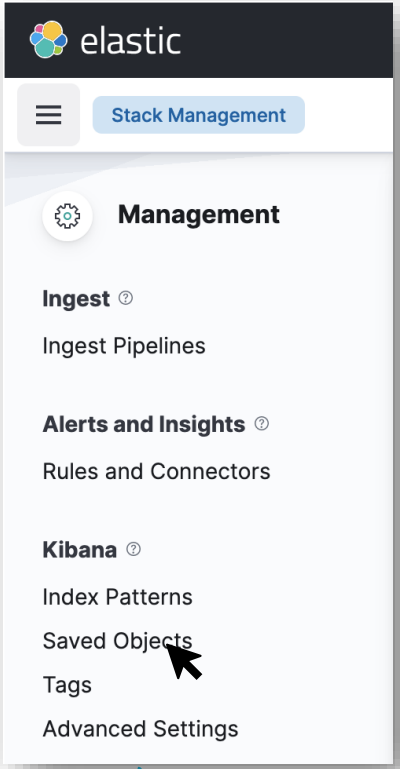
Log Analytics

Index Patterns - Create



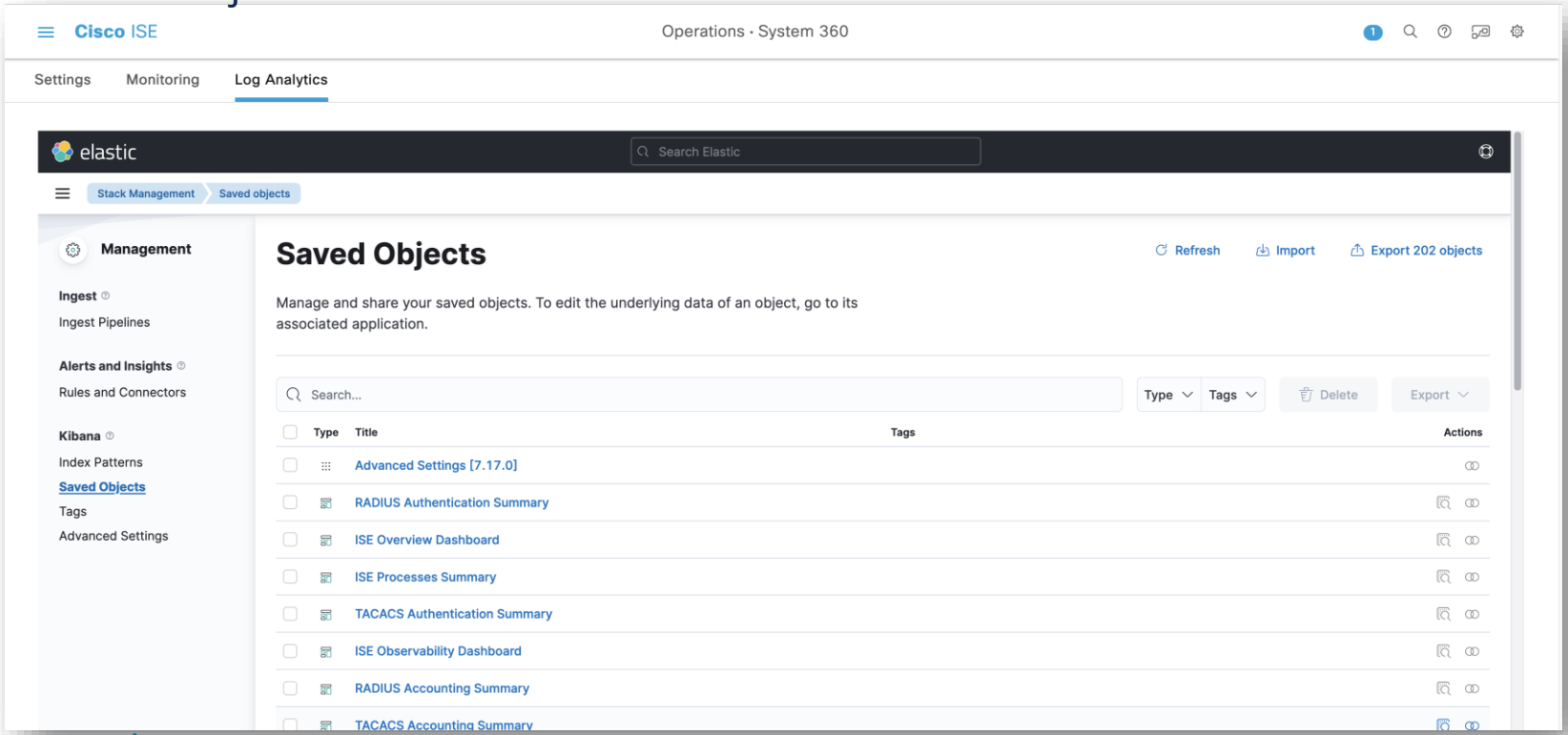
Log Analytics

Menu – Saved Objects



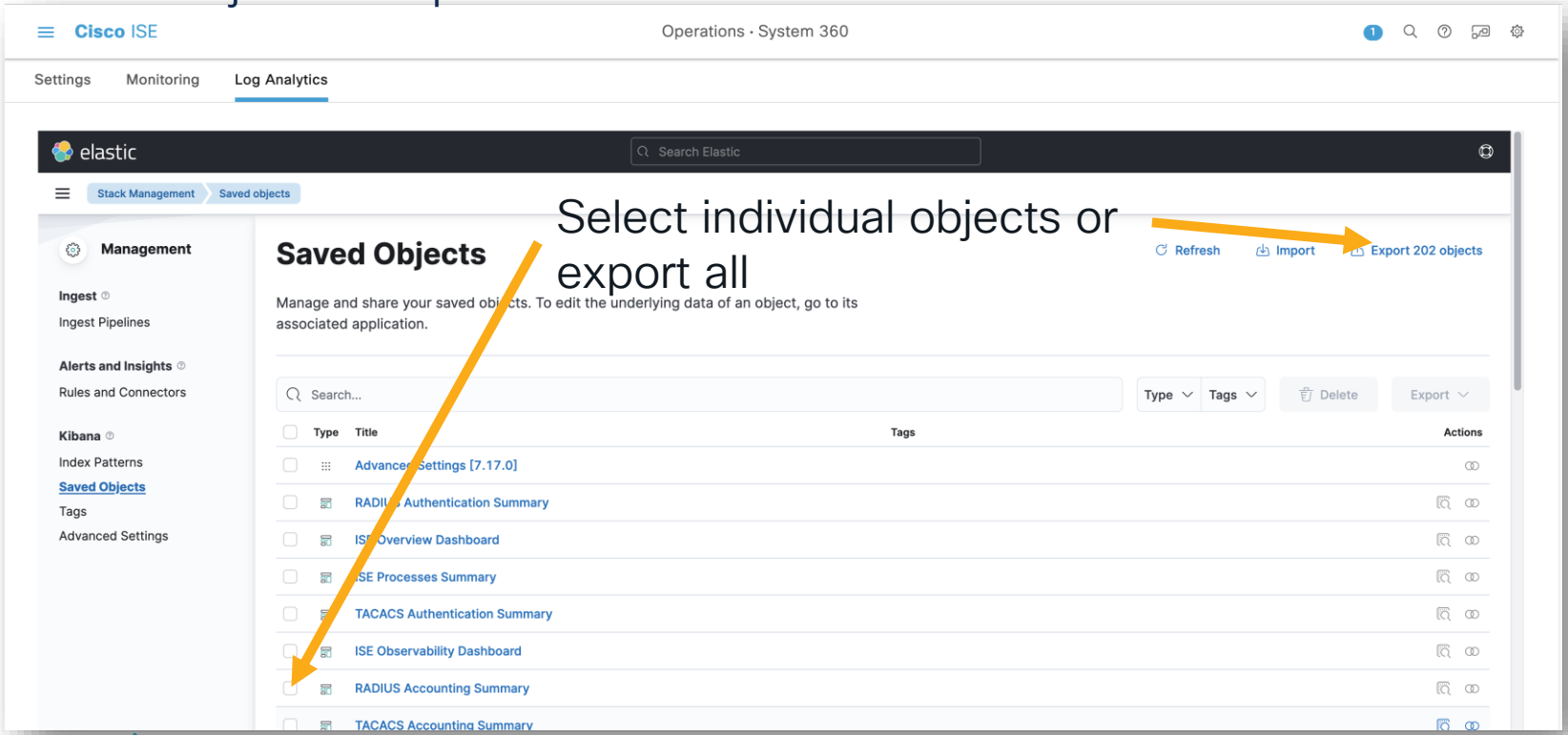
Log Analytics

Saved Objects - Menu



Log Analytics

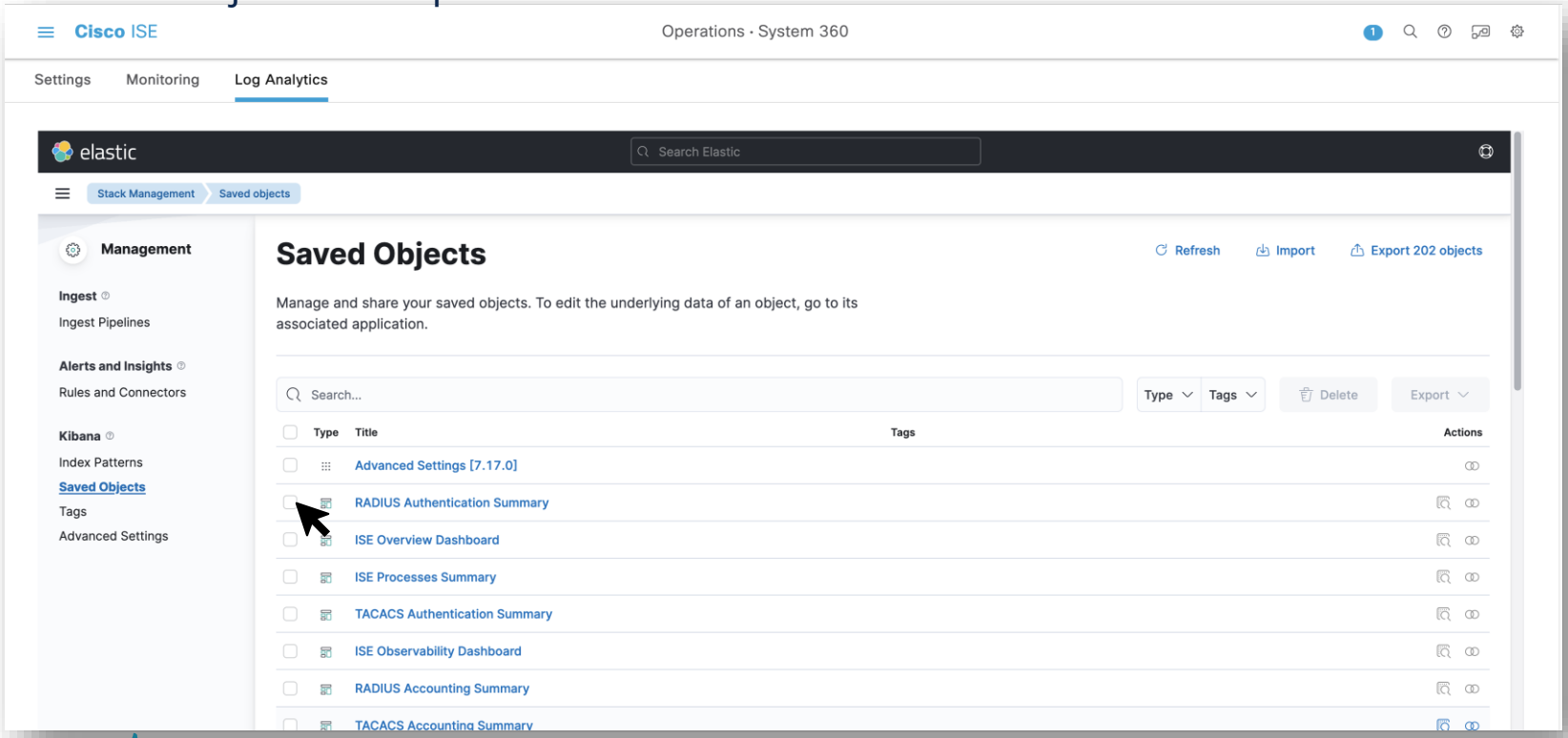
Saved Objects – Export



Select individual objects or export all

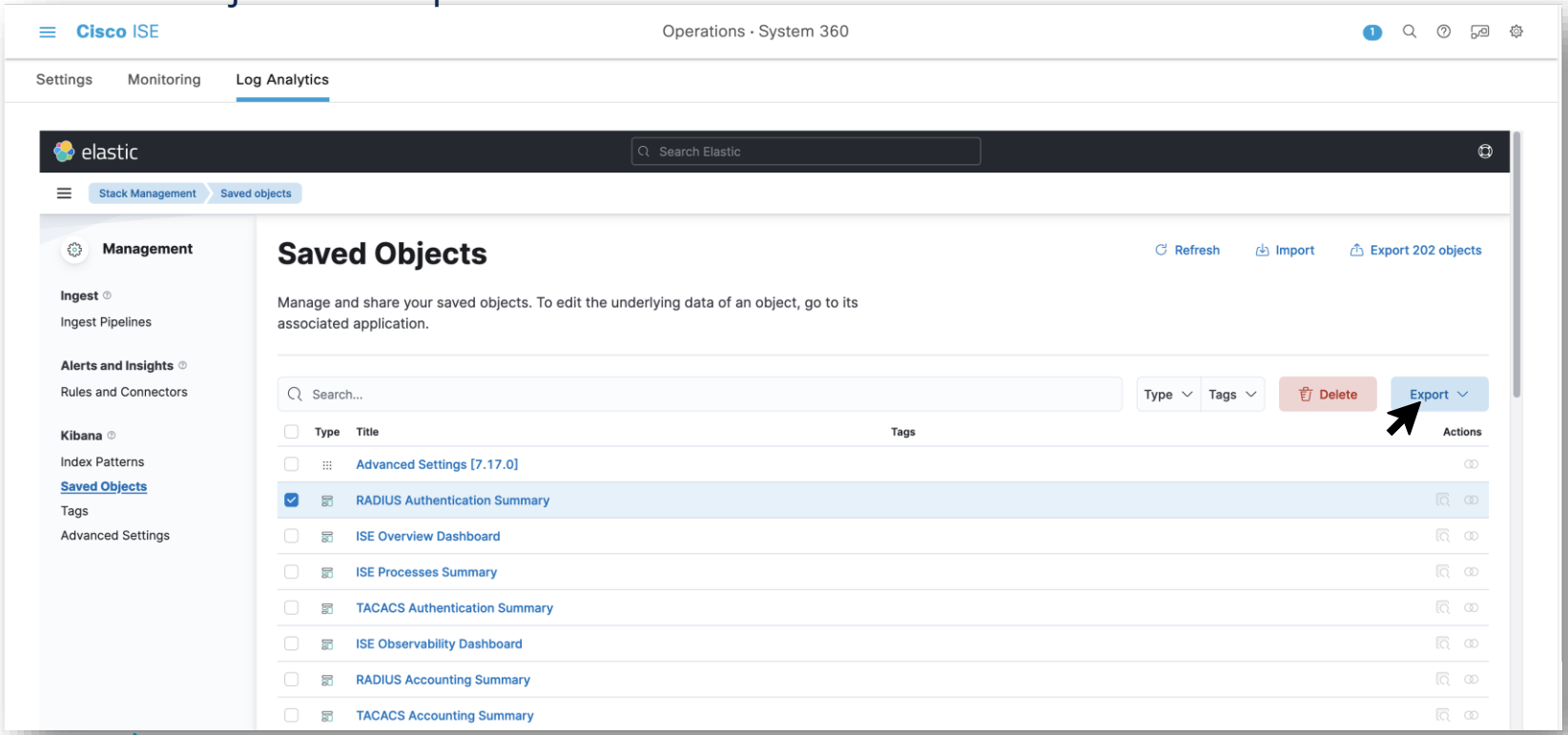
Log Analytics

Saved Objects - Export



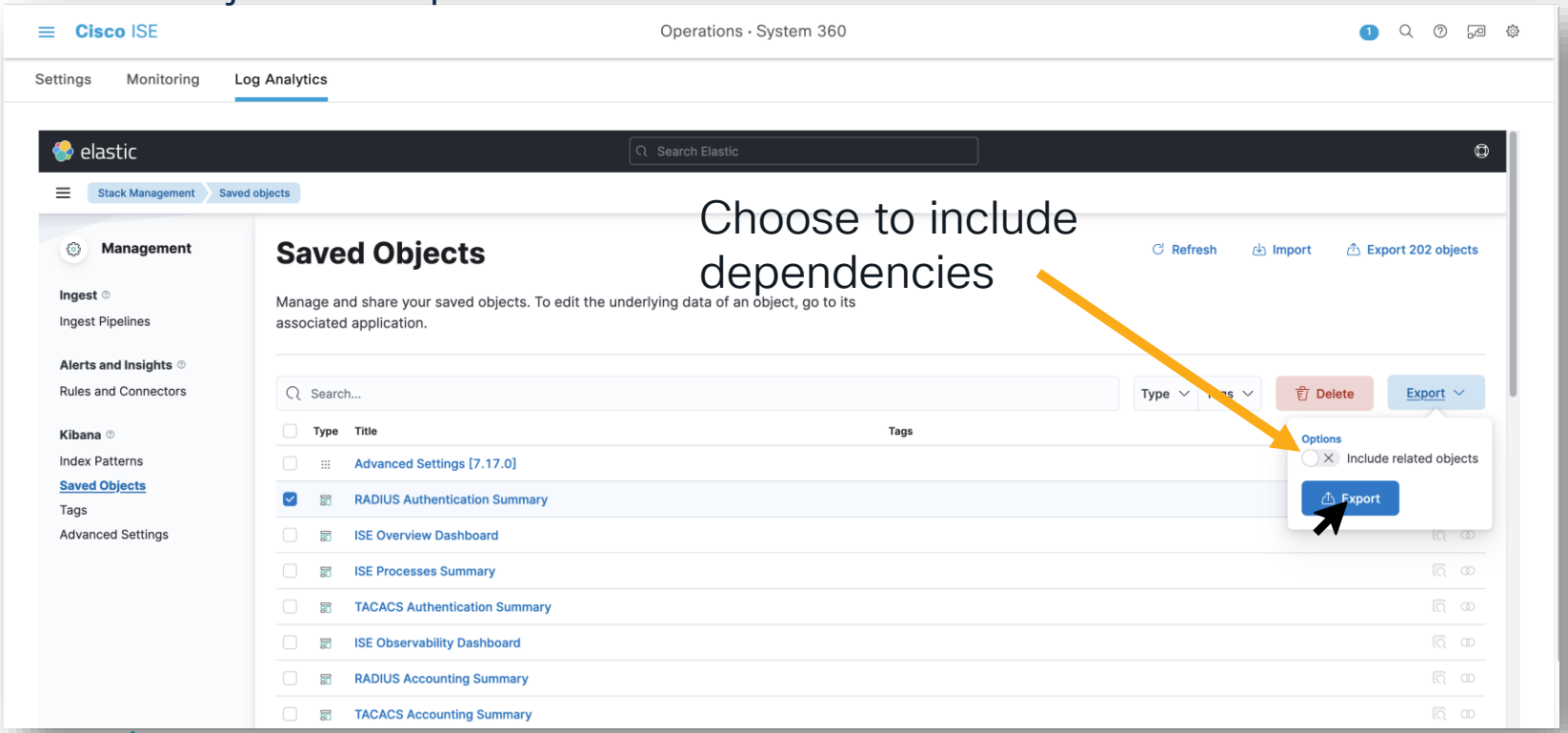
Log Analytics

Saved Objects - Export



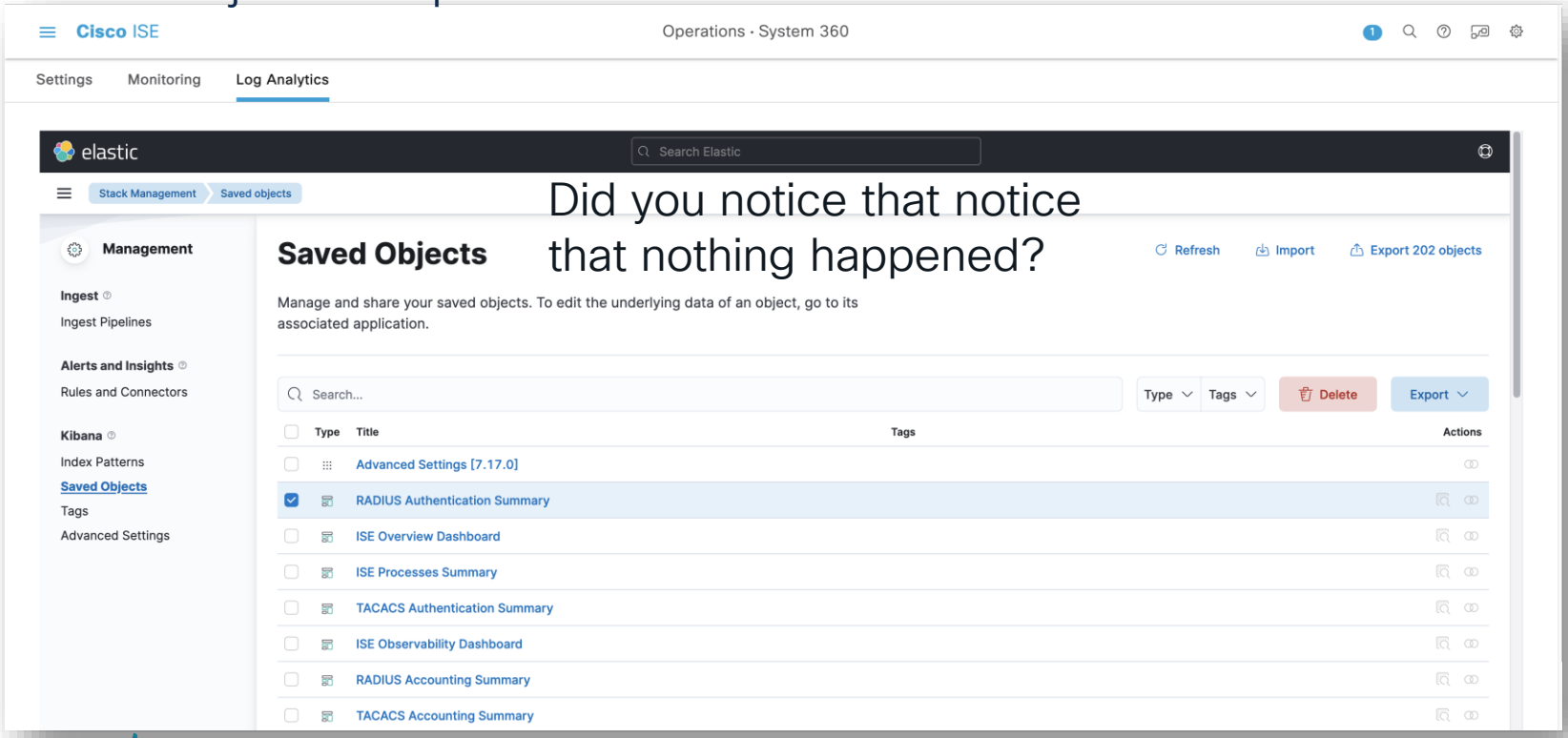
Log Analytics

Saved Objects – Export



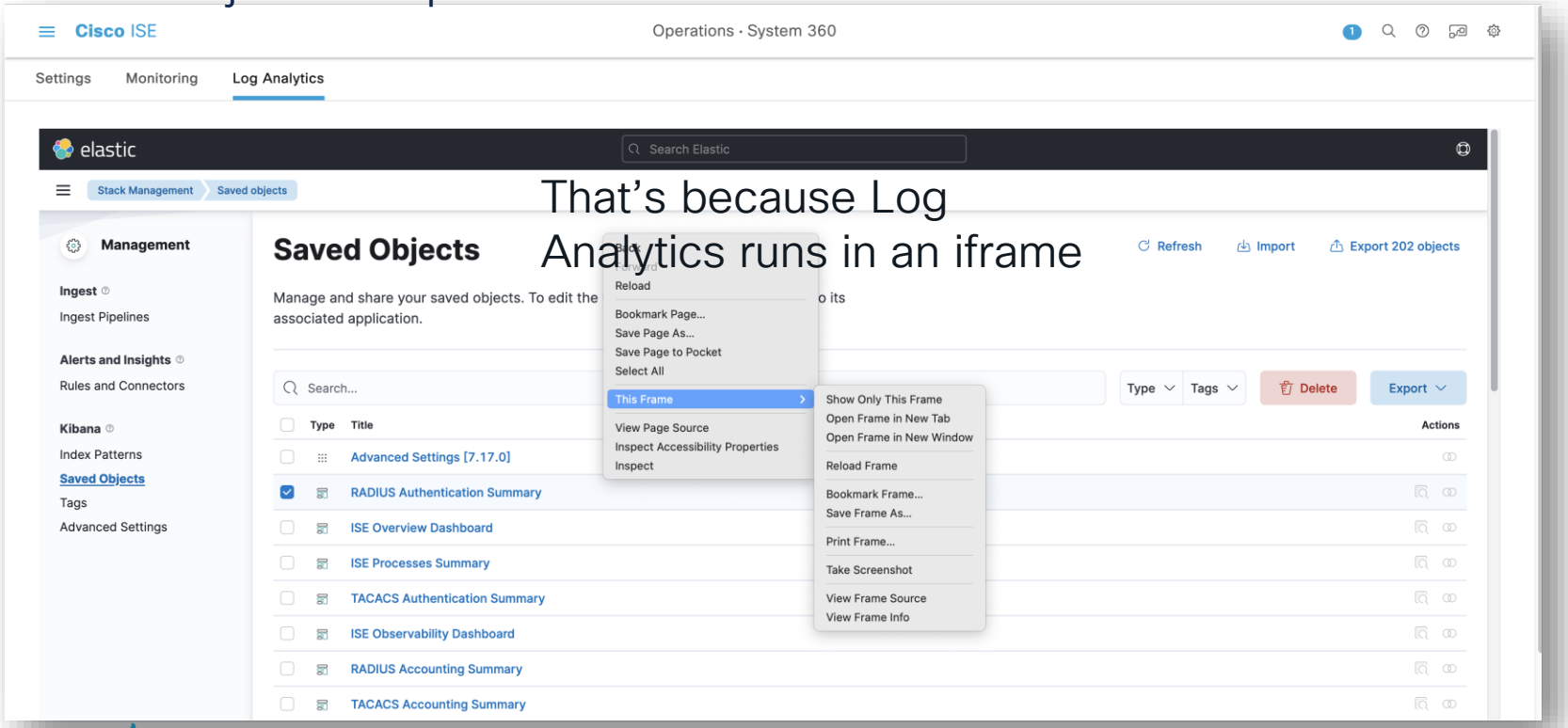
Log Analytics

Saved Objects - Export



Log Analytics

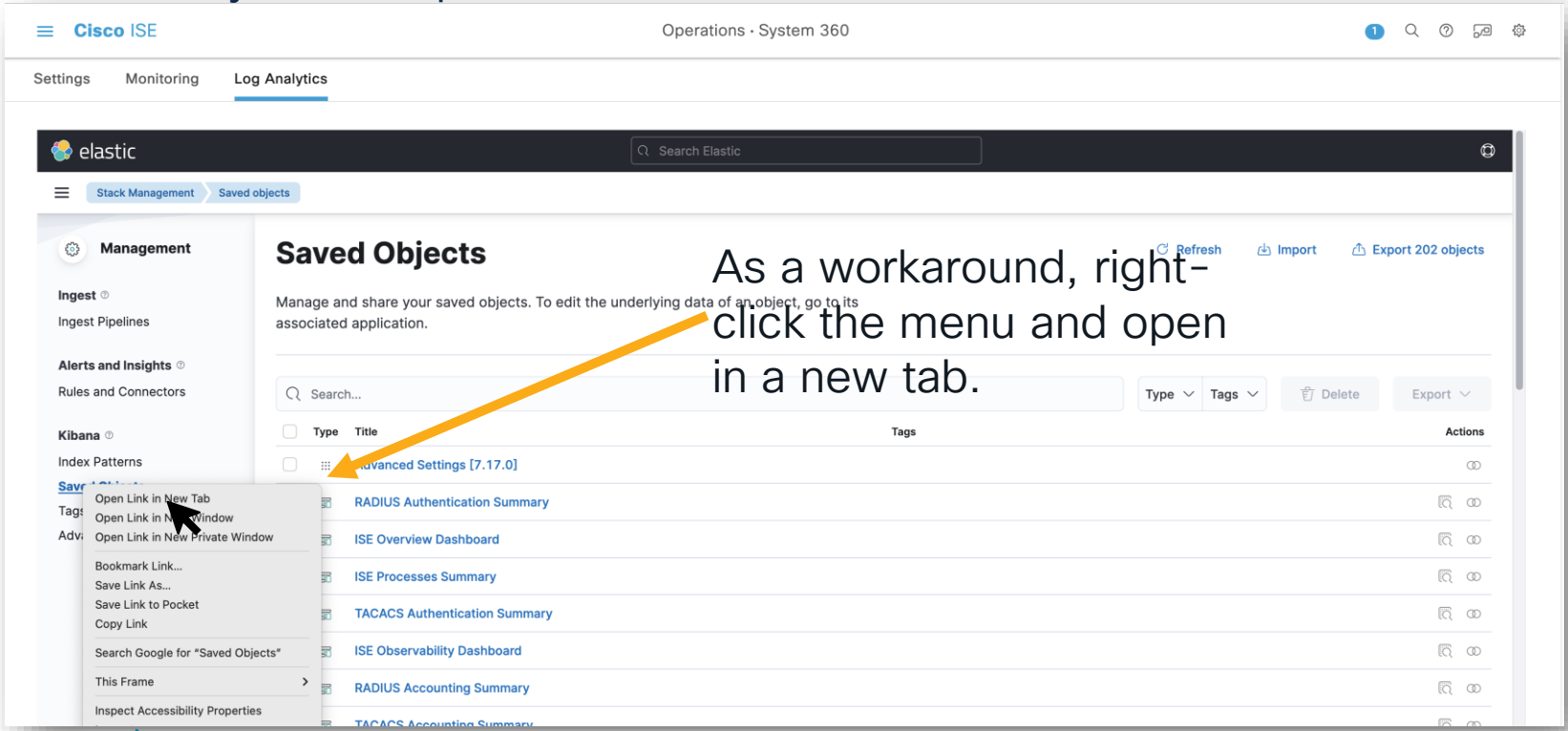
Saved Objects - Export



That's because Log Analytics runs in an iframe

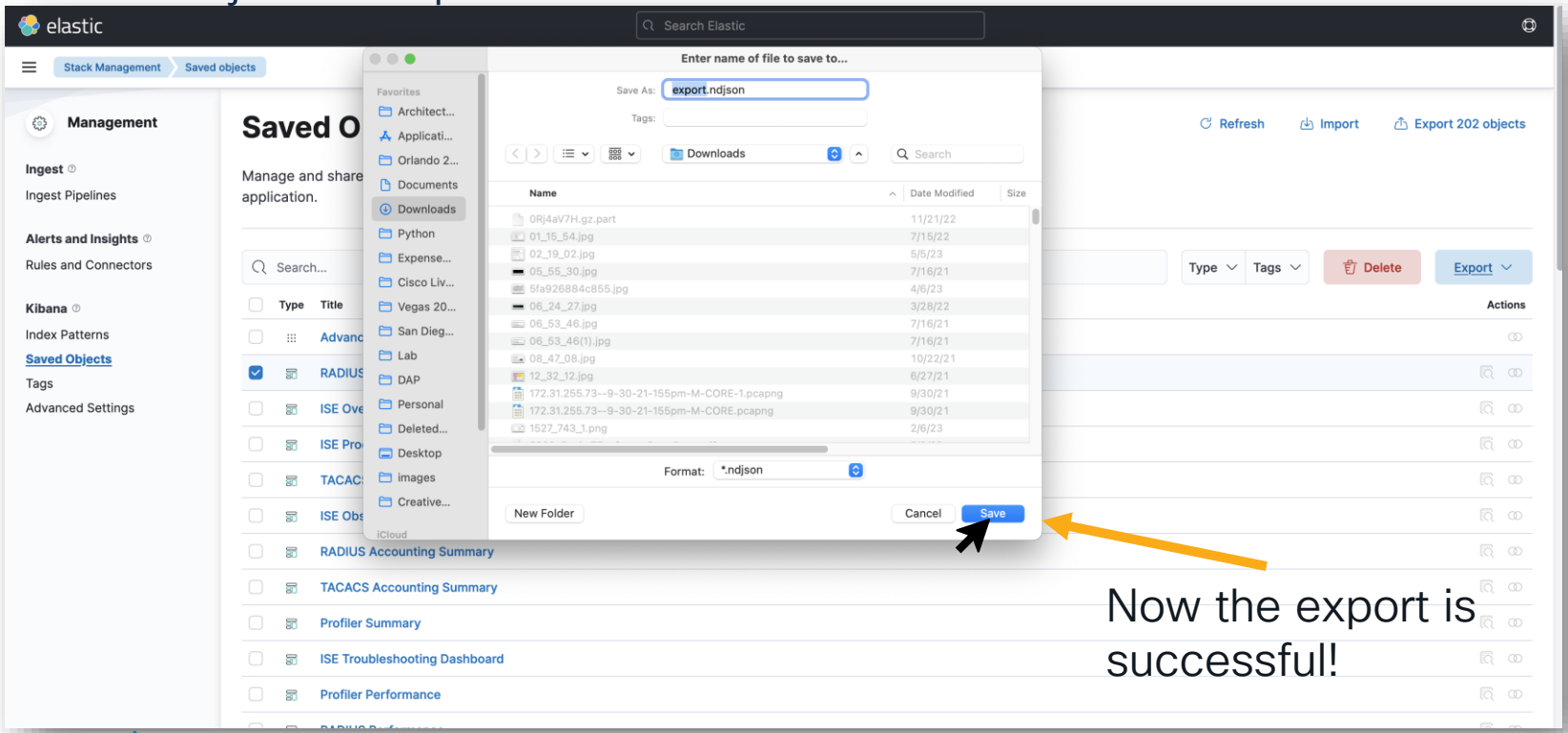
Log Analytics

Saved Objects – Export – Iframe Workaround



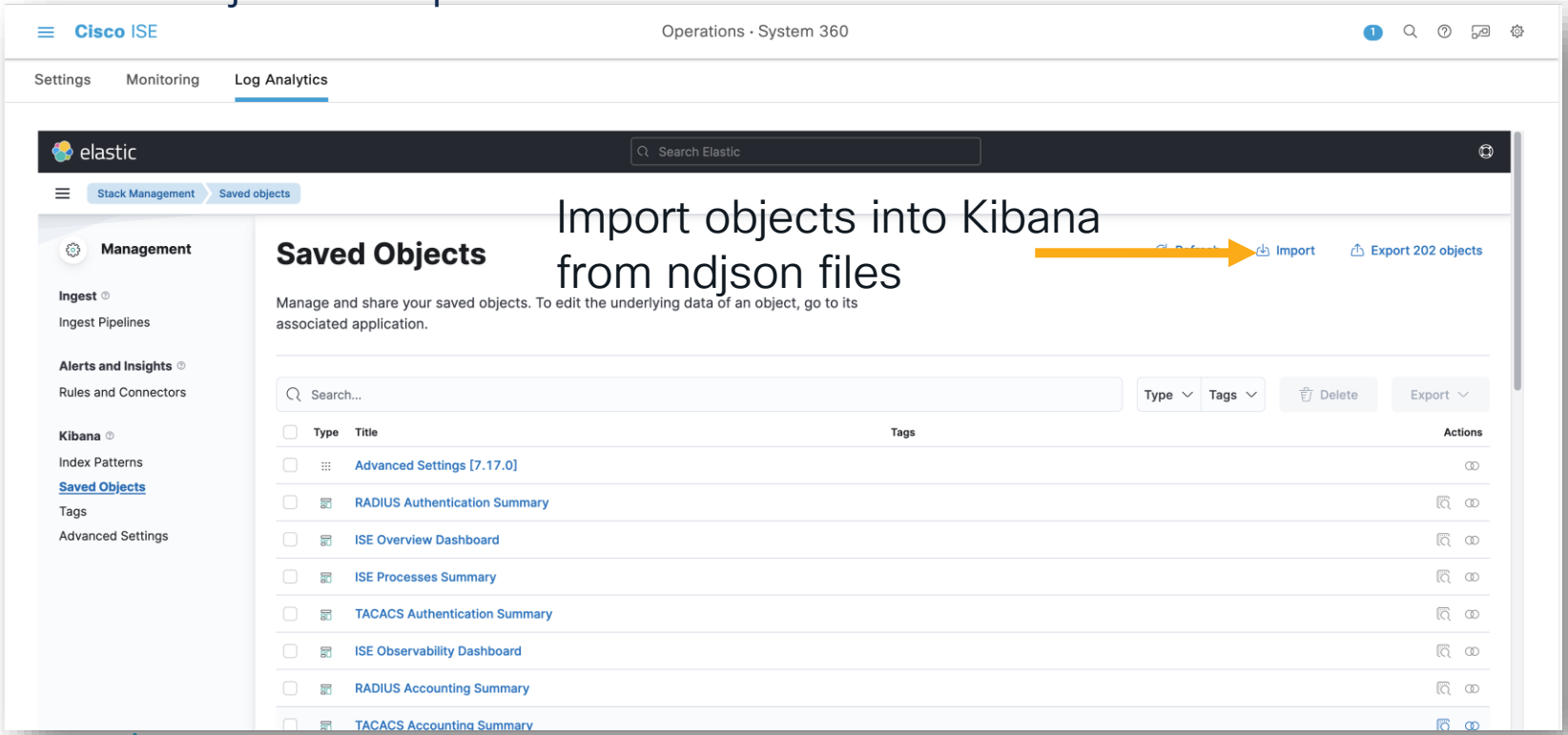
Log Analytics

Saved Objects – Export – Iframe Workaround



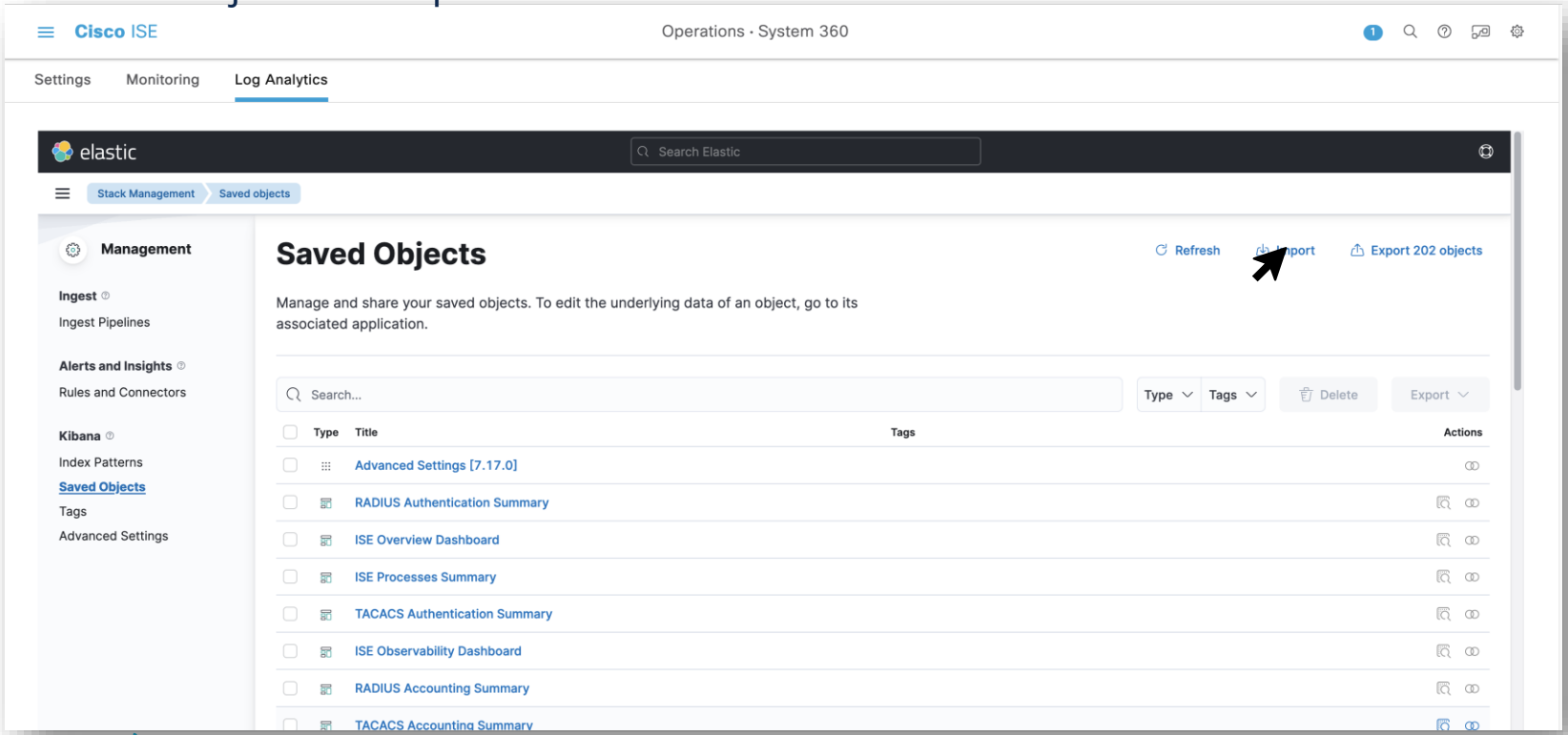
Log Analytics

Saved Objects – Import



Log Analytics

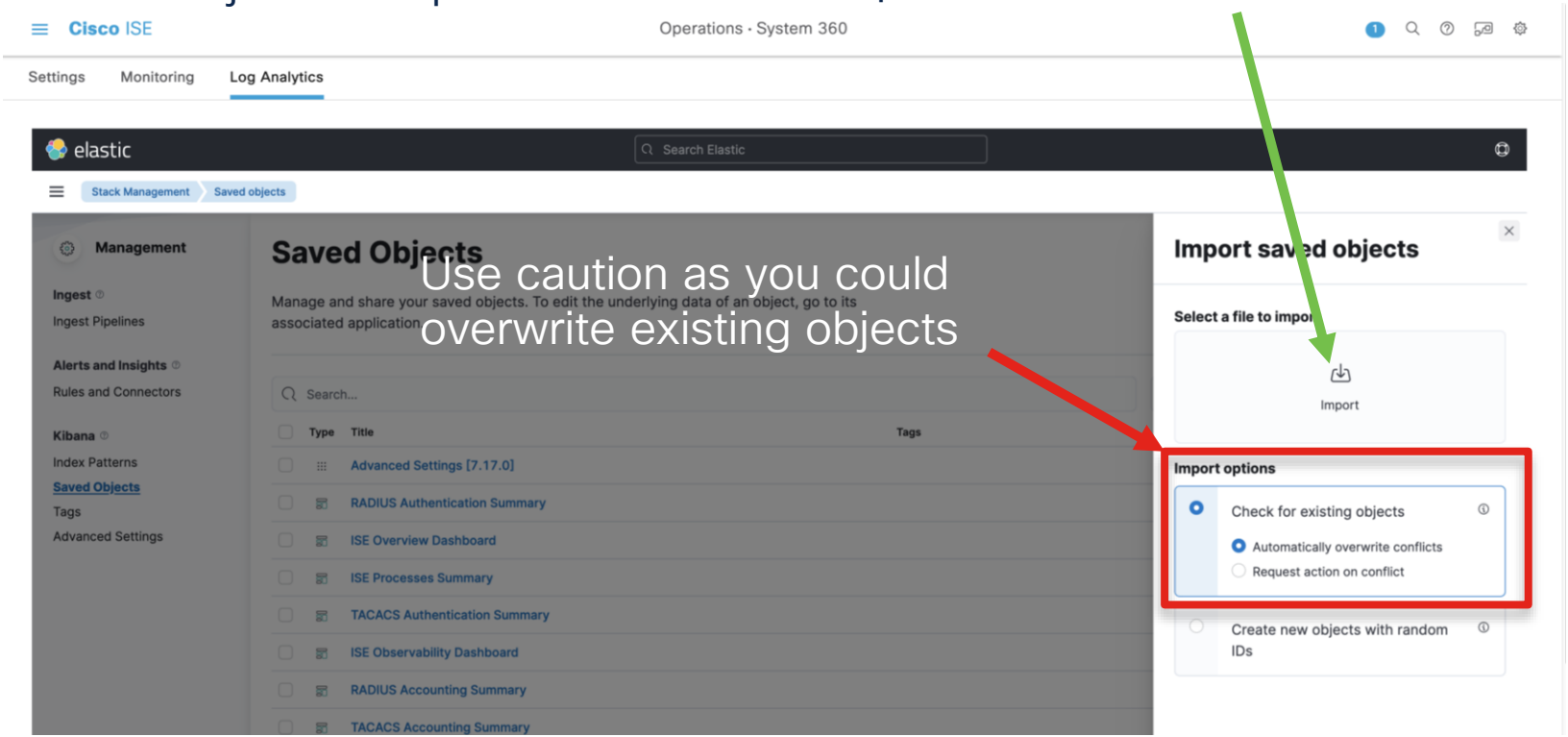
Saved Objects - Import



Log Analytics

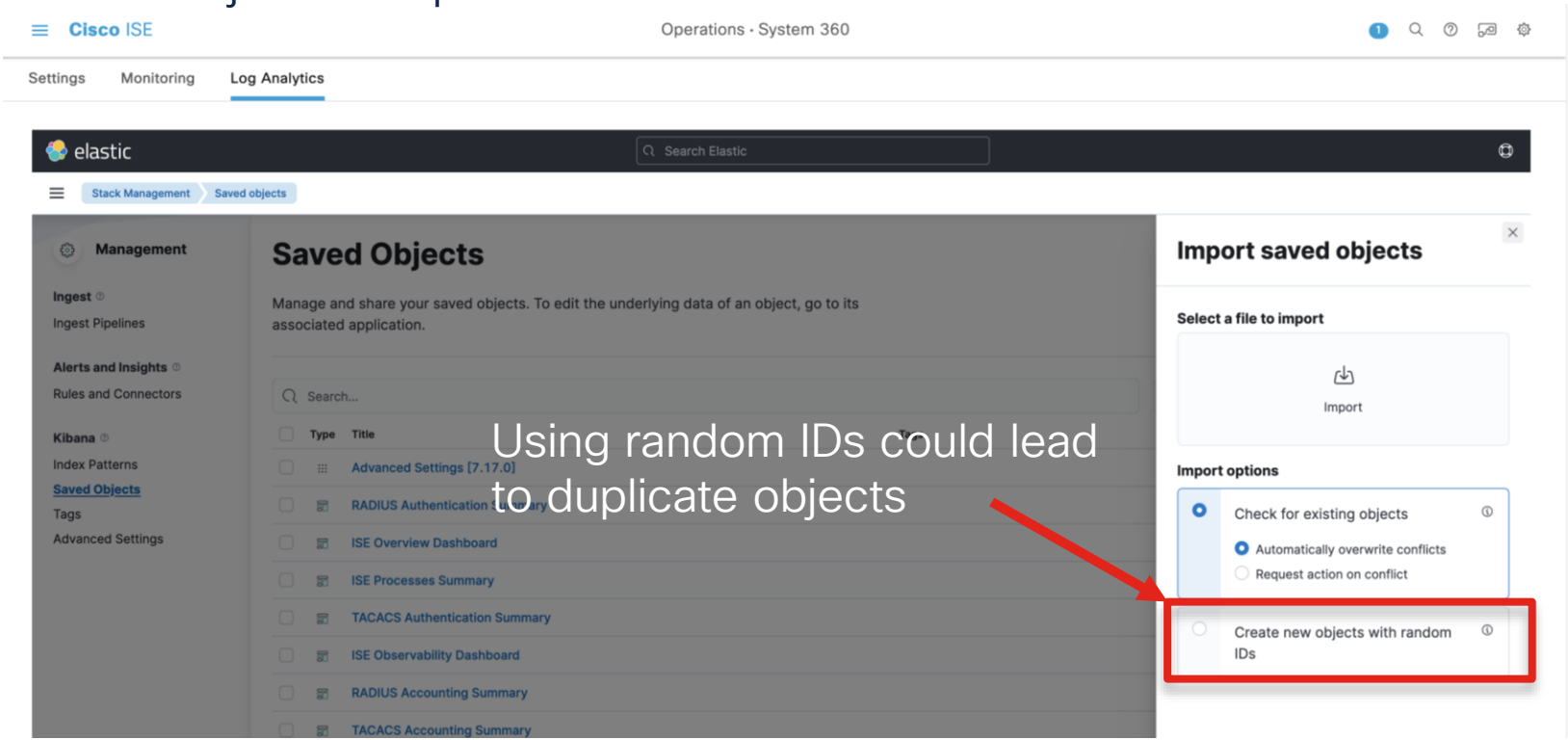
Saved Objects - Import

Import file selection



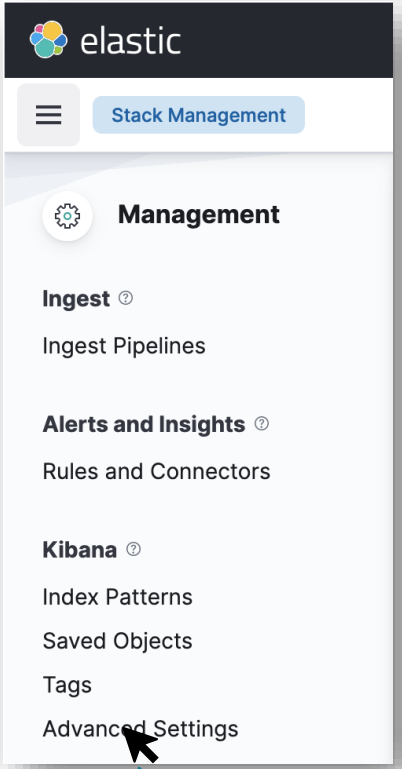
Log Analytics

Saved Objects - Import



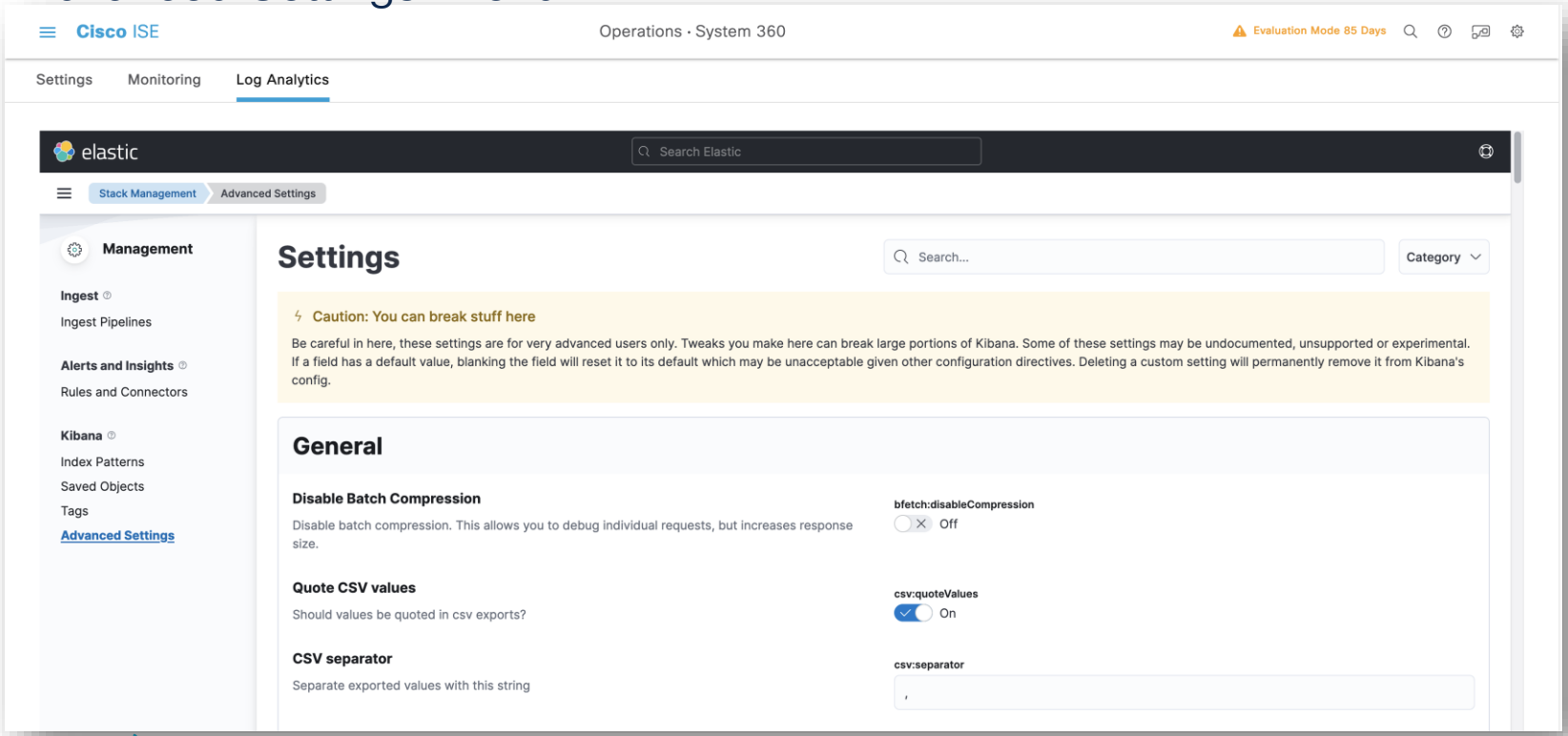
Log Analytics

Menu – Advanced Settings



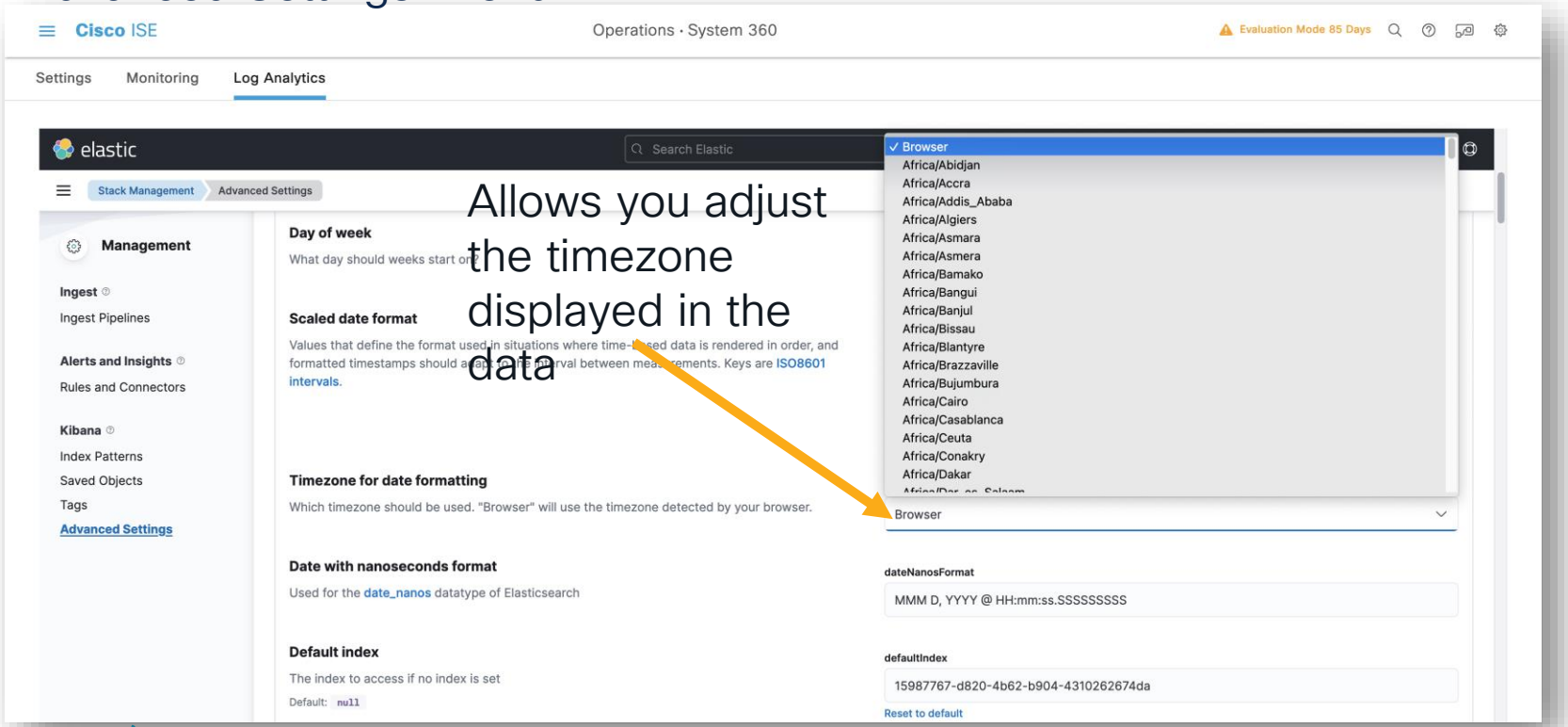
Log Analytics

Advanced Settings-Menu



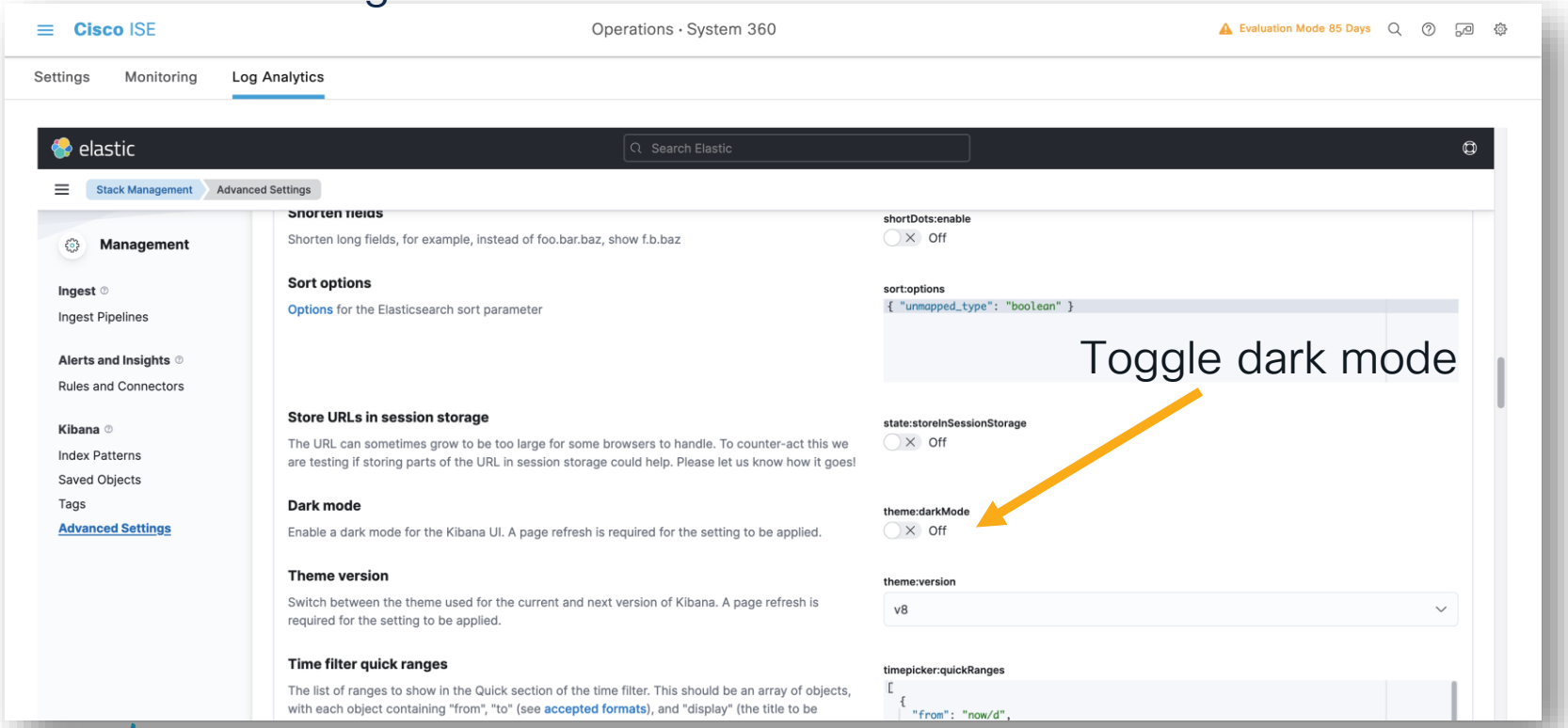
Log Analytics

Advanced Settings-Menu



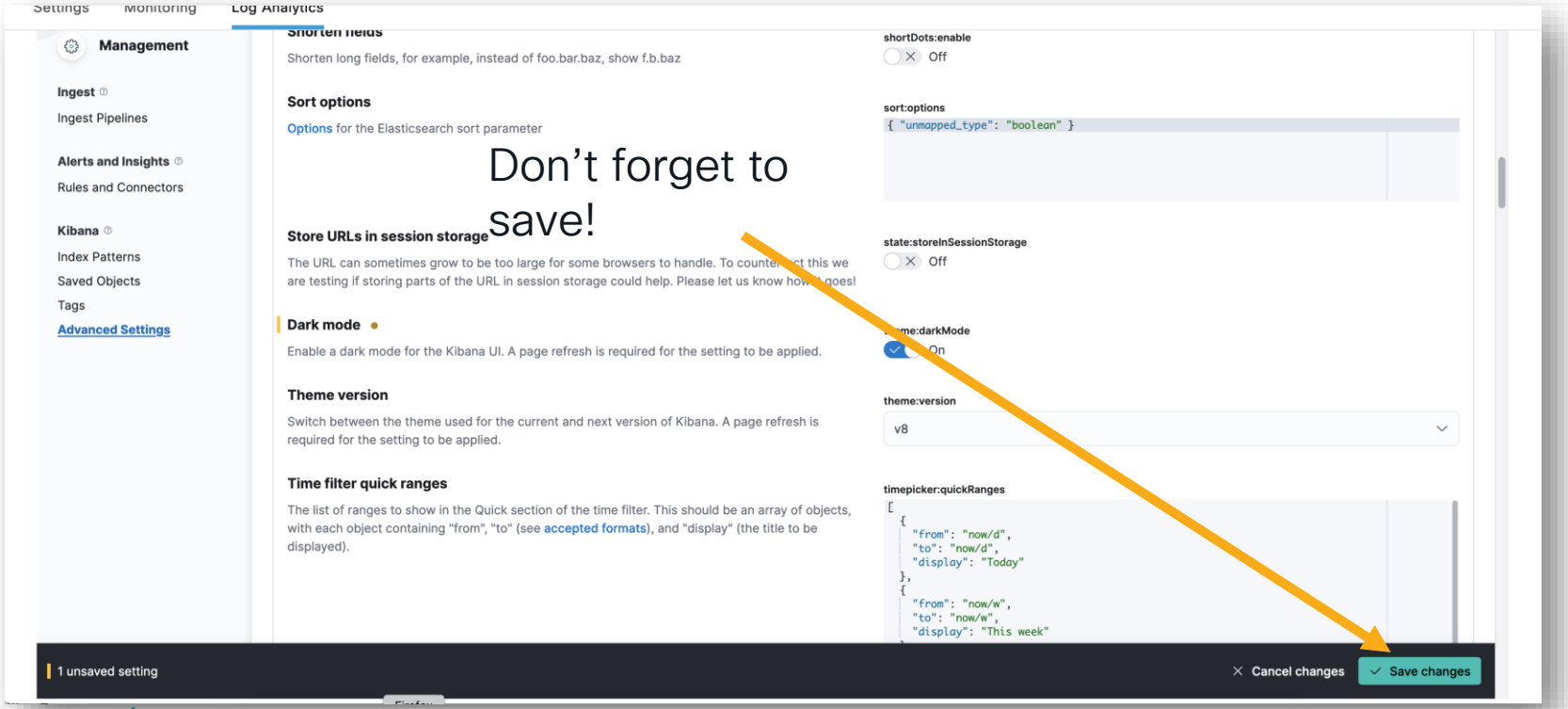
Log Analytics

Advanced Settings-Menu

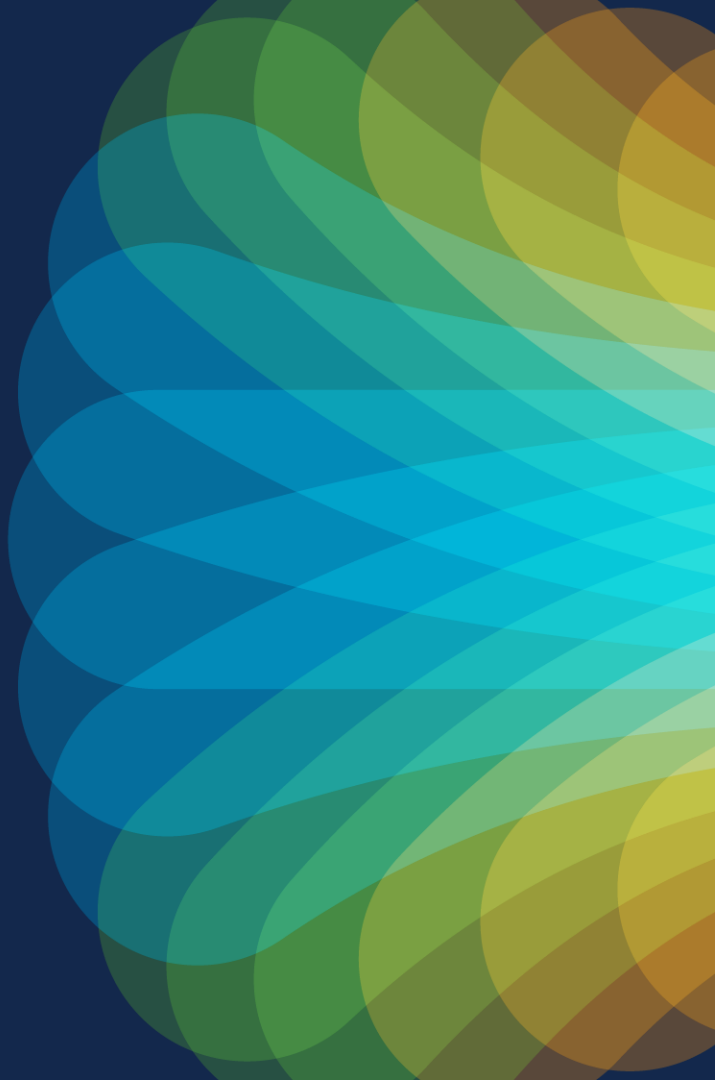


Log Analytics

Advanced Settings-Menu



Demo



Thank You!

cisco Live!


cisco Live!
Let's go
#CiscoLive