Configure Devices to Send and View Troubleshooting Syslogs on FMC

Contents

Introduction

This document describes how to configure managed devices to send diagnostic syslog messages to FMC and view them in the Unified Event Viewer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:
• Syslog Messages
• Firepower Management Center (FMC)
• Firepower Threat Defense (FTD)

Components Used

The information in this document is based on these software and hardware versions:
• This document applies to all Firepower platforms.
• Secure Firewall Threat Defense Virtual (FTD) which runs software version 7.6.0
• Secure Firewall Management Center Virtual (FMC) which runs software version 7.6.0
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Feature Overview

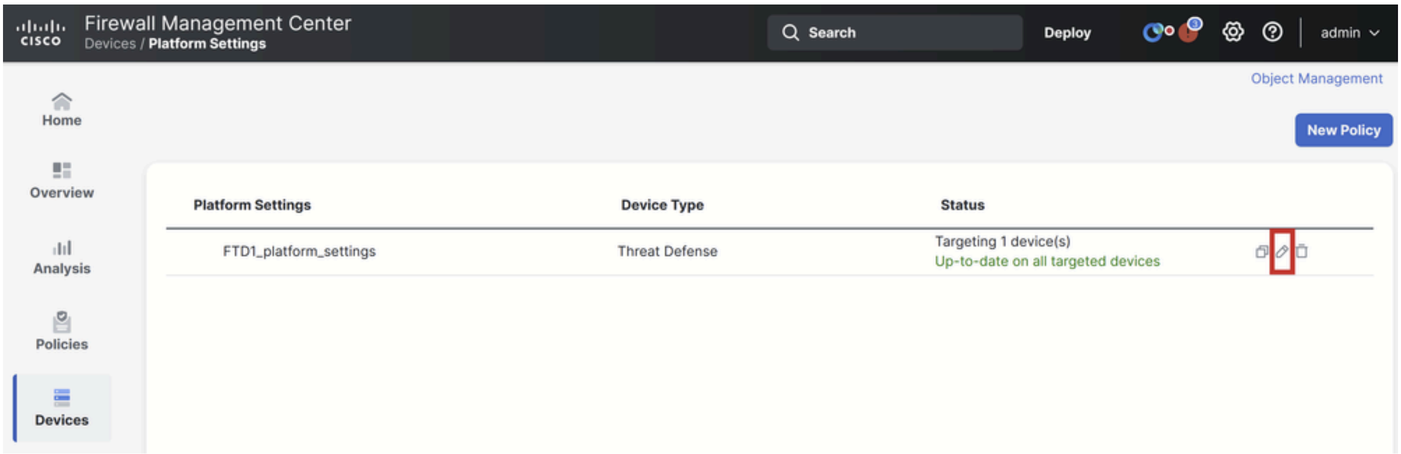
In Secure Firewall 7.6, a new Troubleshoot event type is added in the Unified Event Viewer table. The platform settings syslog logging configuration has been extended and it supports sending LINA generated diagnostic syslog messages to the FMC instead of just VPN logs. This feature can be configured on any FTD running a software version compatible with FMC 7.6.0. cdFMC is not supported because cdFMC does not have analytics tools.

- The All Logs option is limited to emergency, alert, and critical log levels due to event volume.
- These Troubleshooting Logs show any syslog sent from the device to the FMC (VPN or other).
- The troubleshoot logs flow to the FMC and are visible in the Unified Event View and under **Devices >**

Troubleshoot > Troubleshooting Logs.

Configure

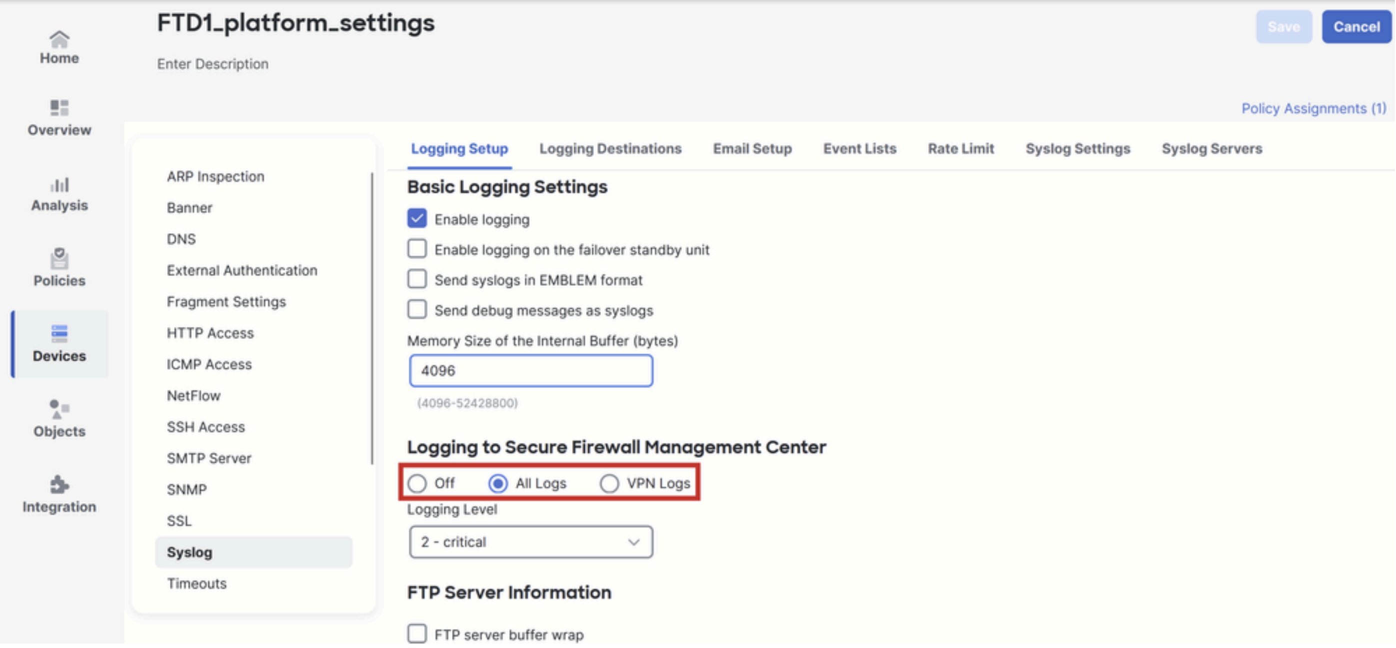
Navigate to **FMC Devices > Platform Settings** and click **Edit** icon at the top right corner of the policy.



Platform Settings	Device Type	Status
FTD1_platform_settings	Threat Defense	Targeting 1 device(s) Up-to-date on all targeted devices

Platform Settings Policy

Move to **Syslog > Logging Setup.** You can see three options under **Logging to Secure Firewall Management Center**.



FTD1_platform_settings

Enter Description

Basic Logging Settings

☑ Enable logging

☐ Enable logging on the failover standby unit

☐ Send syslogs in EMBLEM format

☐ Send debug messages as syslogs

Memory Size of the Internal Buffer (bytes): 4096 (4096-52428800)

Logging to Secure Firewall Management Center

○ Off ● All Logs ○ VPN Logs

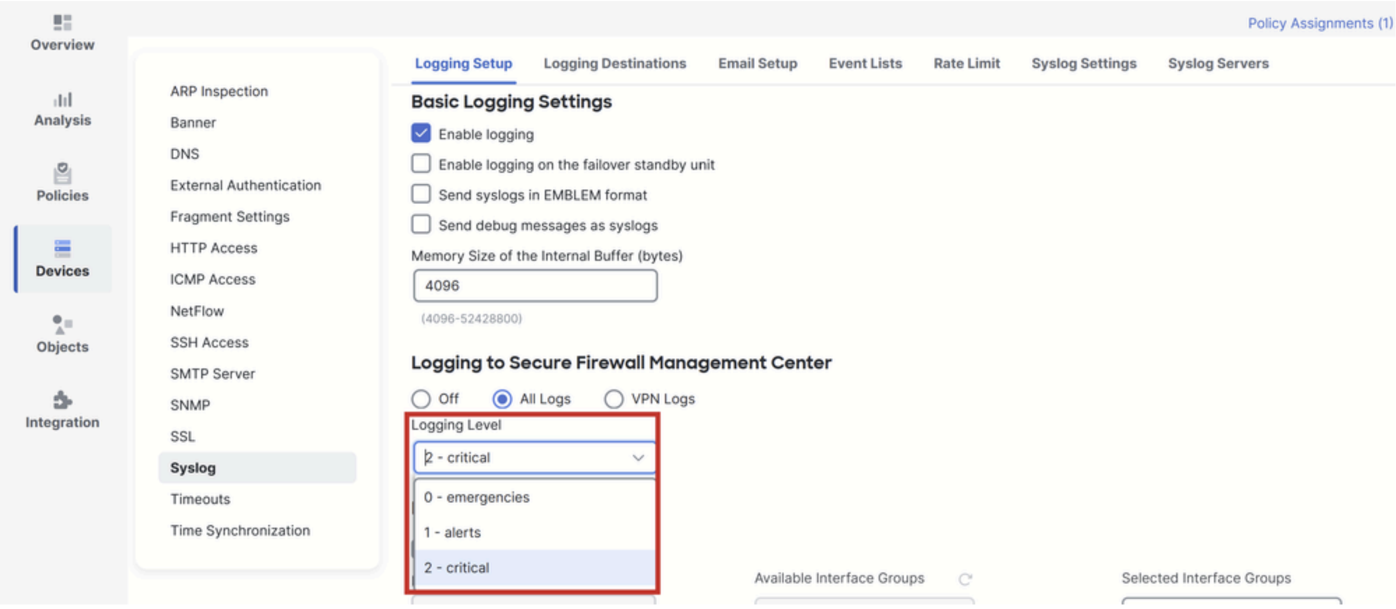
Logging Level: 2 - critical

FTP Server Information

☐ FTP server buffer wrap

Three Logging Options

If you pick **All Logs**, you can select any one of the three logging levels available: emergencies, alerts, and critical and send all diagnostic syslog messages to FMC (including VPN).



Basic Logging Settings

☑ Enable logging

□ Enable logging on the failover standby unit

□ Send syslogs in EMBLEM format

□ Send debug messages as syslogs

Memory Size of the Internal Buffer (bytes)

4096

(4096-52428800)

Logging to Secure Firewall Management Center

○ Off ● All Logs ○ VPN Logs

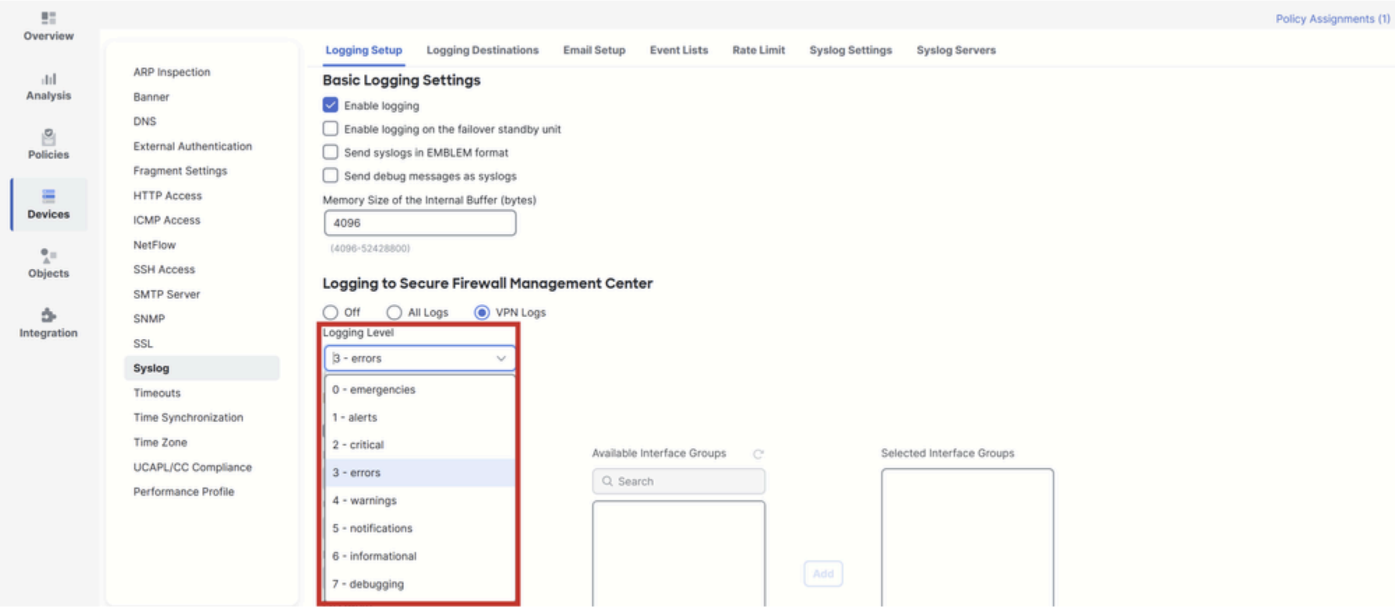
Logging Level

2 - critical

- 0 - emergencies
- 1 - alerts
- 2 - critical

Available Logging Levels

If you pick **VPN Logs**, all logging levels are available and one of those can be selected.



Basic Logging Settings

☑ Enable logging

□ Enable logging on the failover standby unit

□ Send syslogs in EMBLEM format

□ Send debug messages as syslogs

Memory Size of the Internal Buffer (bytes)

4096

(4096-52428800)

Logging to Secure Firewall Management Center

○ Off ○ All Logs ● VPN Logs

Logging Level

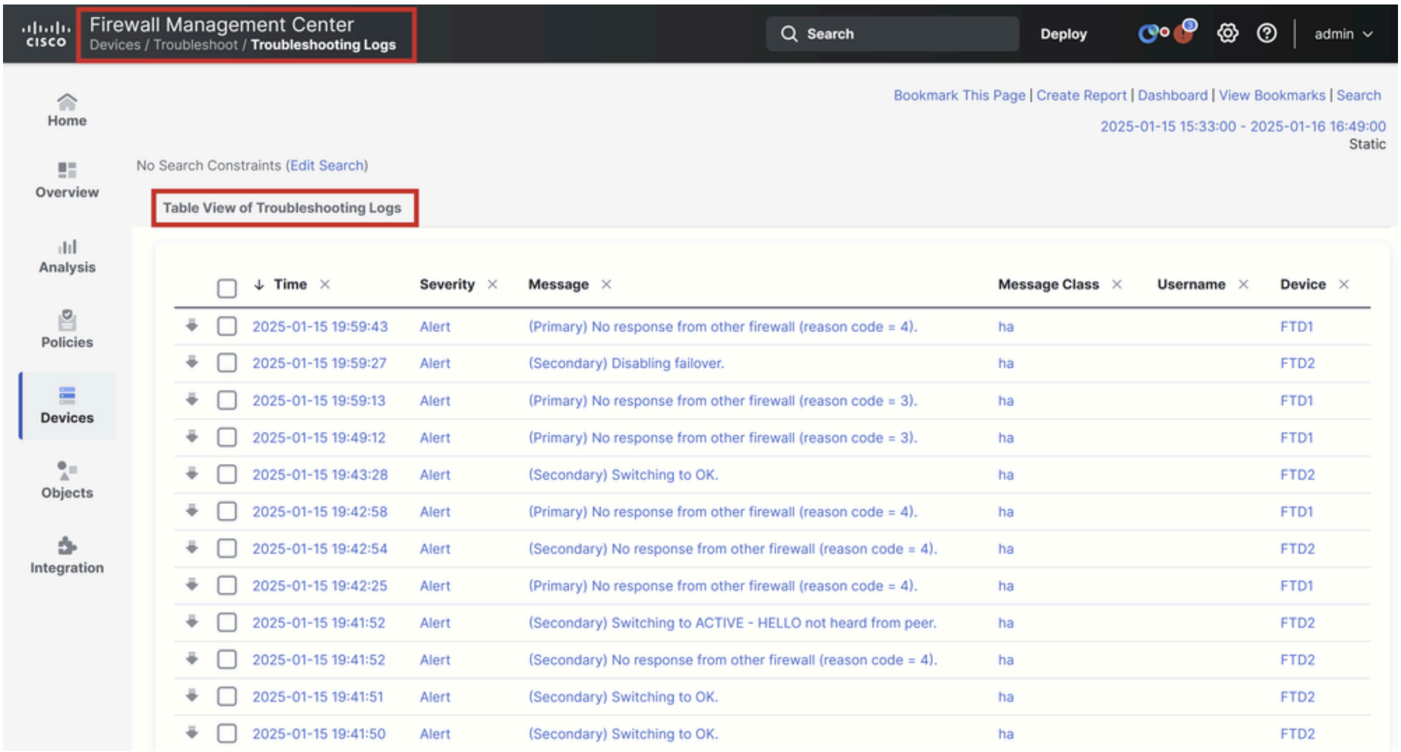
3 - errors

- 0 - emergencies
- 1 - alerts
- 2 - critical
- 3 - errors
- 4 - warnings
- 5 - notifications
- 6 - informational
- 7 - debugging

Available Logging Levels

Note: When you configure a device with site-to-site or remote access VPN, it automatically enables sending VPN syslogs to the management center by default. You can change it to All Logs to send all syslogs besides VPN logs to FMC.

These logs can be accessed from **Devices > Troubleshoot > Troubleshooting Logs**.



Firewall Management Center
Devices / Troubleshoot / Troubleshooting Logs
Search
Deploy
admin
Home
Overview
Analysis
Policies
Devices
Objects
Integration
Bookmark This Page | Create Report | Dashboard | View Bookmarks | Search

2025-01-15 15:33:00 - 2025-01-16 16:49:00
Static

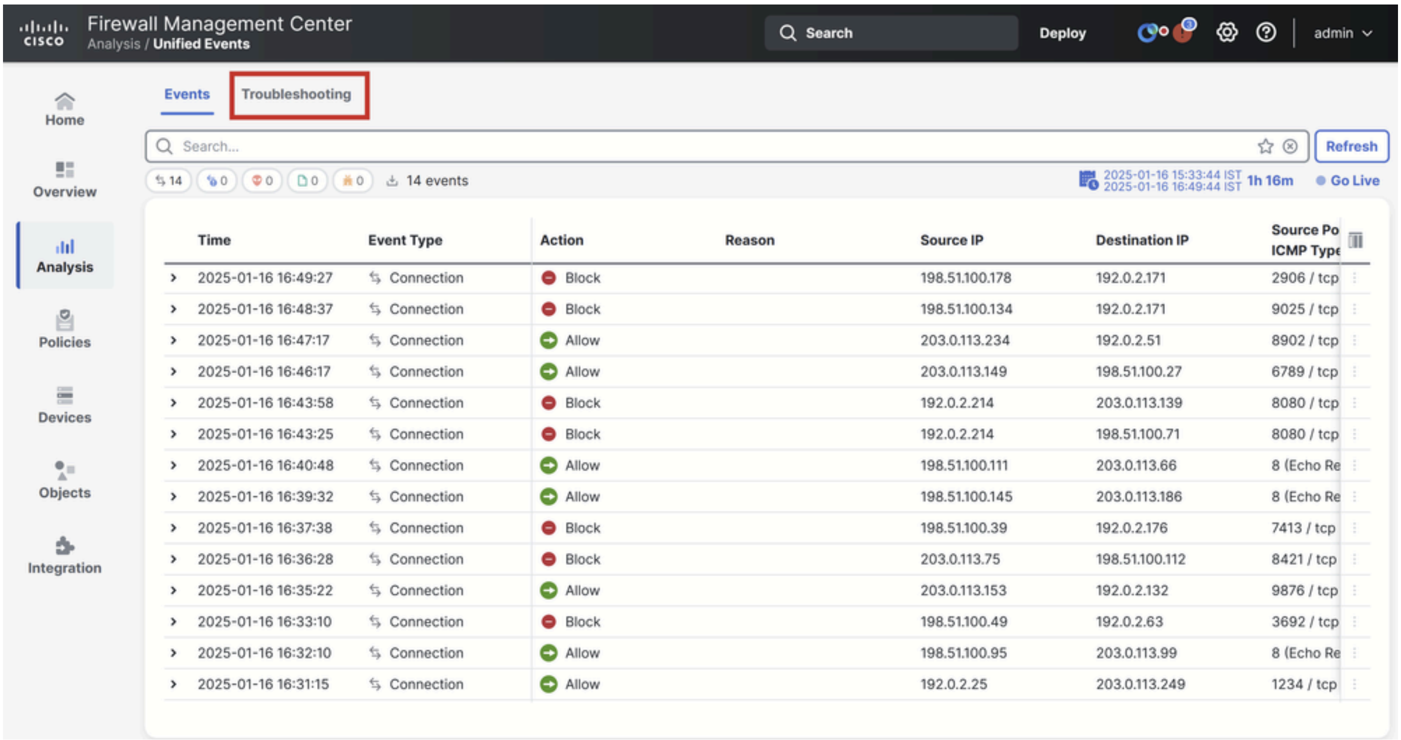
No Search Constraints (Edit Search)

Table View of Troubleshooting Logs

	Time	Severity	Message	Message Class	Username	Device
□	2025-01-15 19:59:43	Alert	(Primary) No response from other firewall (reason code = 4).	ha		FTD1
□	2025-01-15 19:59:27	Alert	(Secondary) Disabling failover.	ha		FTD2
□	2025-01-15 19:59:13	Alert	(Primary) No response from other firewall (reason code = 3).	ha		FTD1
□	2025-01-15 19:49:12	Alert	(Primary) No response from other firewall (reason code = 3).	ha		FTD1
□	2025-01-15 19:43:28	Alert	(Secondary) Switching to OK.	ha		FTD2
□	2025-01-15 19:42:58	Alert	(Primary) No response from other firewall (reason code = 4).	ha		FTD1
□	2025-01-15 19:42:54	Alert	(Secondary) No response from other firewall (reason code = 4).	ha		FTD2
□	2025-01-15 19:42:25	Alert	(Primary) No response from other firewall (reason code = 4).	ha		FTD1
□	2025-01-15 19:41:52	Alert	(Secondary) Switching to ACTIVE - HELLO not heard from peer.	ha		FTD2
□	2025-01-15 19:41:52	Alert	(Secondary) No response from other firewall (reason code = 4).	ha		FTD2
□	2025-01-15 19:41:51	Alert	(Secondary) Switching to OK.	ha		FTD2
□	2025-01-15 19:41:50	Alert	(Secondary) Switching to OK.	ha		FTD2

Table View of Troubleshooting Logs

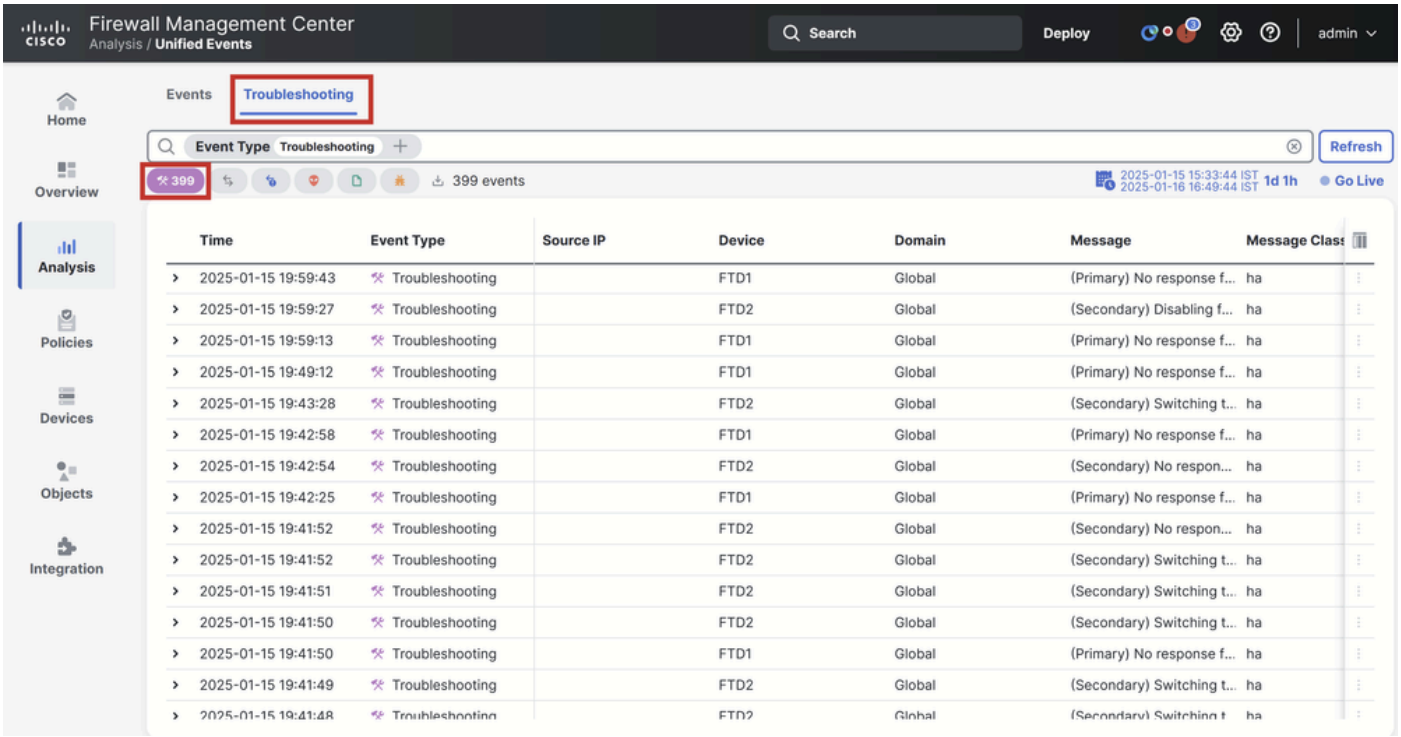
A new Troubleshooting view tab is now available on the Unified Event Viewer page. To view these events, navigate to **Analysis > Unified Events > Troubleshooting**.



Time	Event Type	Action	Reason	Source IP	Destination IP	Source Po ICMP Type
2025-01-16 16:49:27	Connection	Block		198.51.100.178	192.0.2.171	2906 / tcp
2025-01-16 16:48:37	Connection	Block		198.51.100.134	192.0.2.171	9025 / tcp
2025-01-16 16:47:17	Connection	Allow		203.0.113.234	192.0.2.51	8902 / tcp
2025-01-16 16:46:17	Connection	Allow		203.0.113.149	198.51.100.27	6789 / tcp
2025-01-16 16:43:58	Connection	Block		192.0.2.214	203.0.113.139	8080 / tcp
2025-01-16 16:43:25	Connection	Block		192.0.2.214	198.51.100.71	8080 / tcp
2025-01-16 16:40:48	Connection	Allow		198.51.100.111	203.0.113.66	8 (Echo Re
2025-01-16 16:39:32	Connection	Allow		198.51.100.145	203.0.113.186	8 (Echo Re
2025-01-16 16:37:38	Connection	Block		198.51.100.39	192.0.2.176	7413 / tcp
2025-01-16 16:36:28	Connection	Block		203.0.113.75	198.51.100.112	8421 / tcp
2025-01-16 16:35:22	Connection	Allow		203.0.113.153	192.0.2.132	9876 / tcp
2025-01-16 16:33:10	Connection	Block		198.51.100.49	192.0.2.63	3692 / tcp
2025-01-16 16:32:10	Connection	Allow		198.51.100.95	203.0.113.99	8 (Echo Re
2025-01-16 16:31:15	Connection	Allow		192.0.2.25	203.0.113.249	1234 / tcp

Troubleshooting View

A new event type is visible within the table once you switch to this tab. It cannot be added or removed from the view like the other types since it is central to the **Troubleshooting view.**



Event Type Troubleshooting

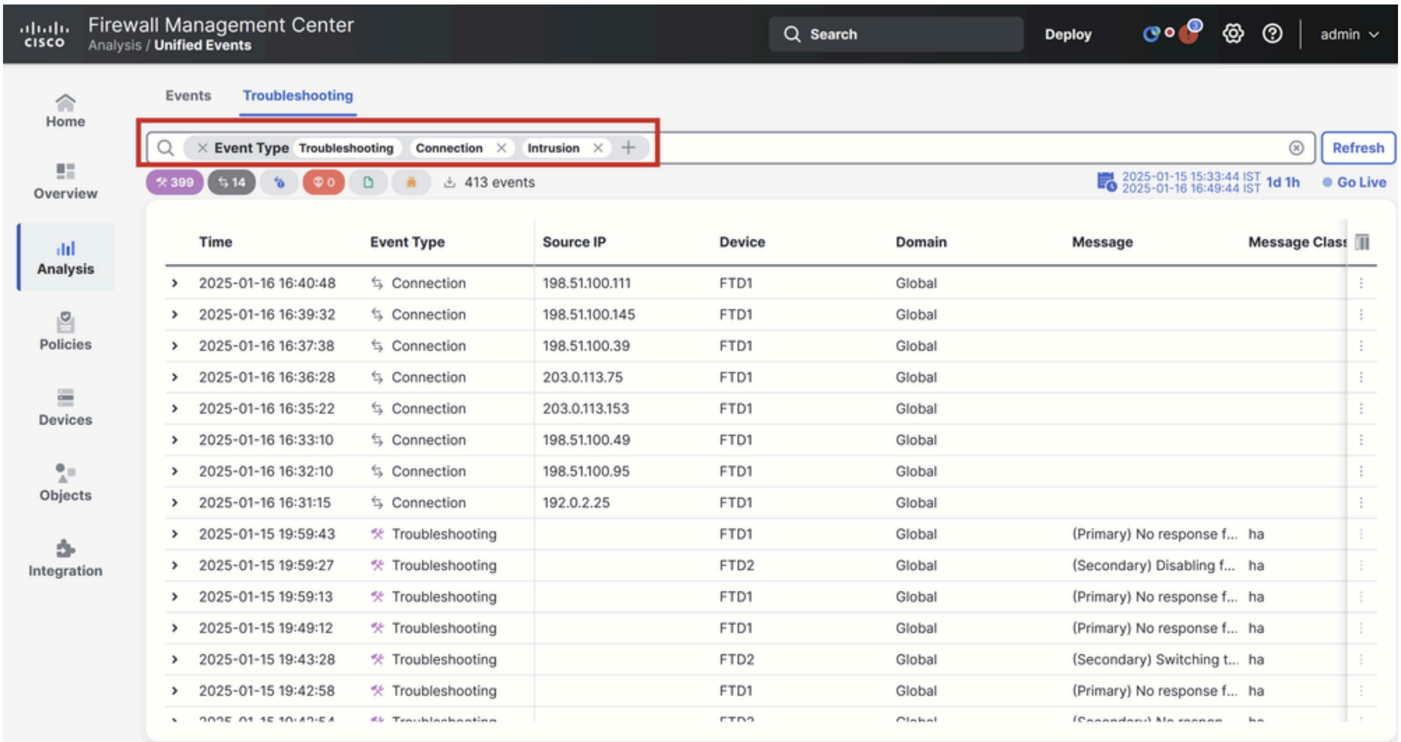
399 · 399 events

2025-01-15 15:33:44 IST – 2025-01-16 16:49:44 IST · 1d 1h

Time	Event Type	Source IP	Device	Domain	Message	Message Class
2025-01-15 19:59:43	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:59:27	Troubleshooting		FTD2	Global	(Secondary) Disabling f...	ha
2025-01-15 19:59:13	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:49:12	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:43:28	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
2025-01-15 19:42:58	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:42:54	Troubleshooting		FTD2	Global	(Secondary) No respon...	ha
2025-01-15 19:42:25	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:41:52	Troubleshooting		FTD2	Global	(Secondary) No respon...	ha
2025-01-15 19:41:52	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
2025-01-15 19:41:51	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
2025-01-15 19:41:50	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
2025-01-15 19:41:50	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:41:49	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
2025-01-15 19:41:48	Troubleshooting		FTD2	Global	(Secondary) Switching t	ha

Troubleshooting Event Type

Other event types can still be added and removed from this Troubleshooting view. This allows you to view diagnostic logs alongside other event data.



Event Type Troubleshooting Connection Intrusion

399 · 14 · 0 · 413 events

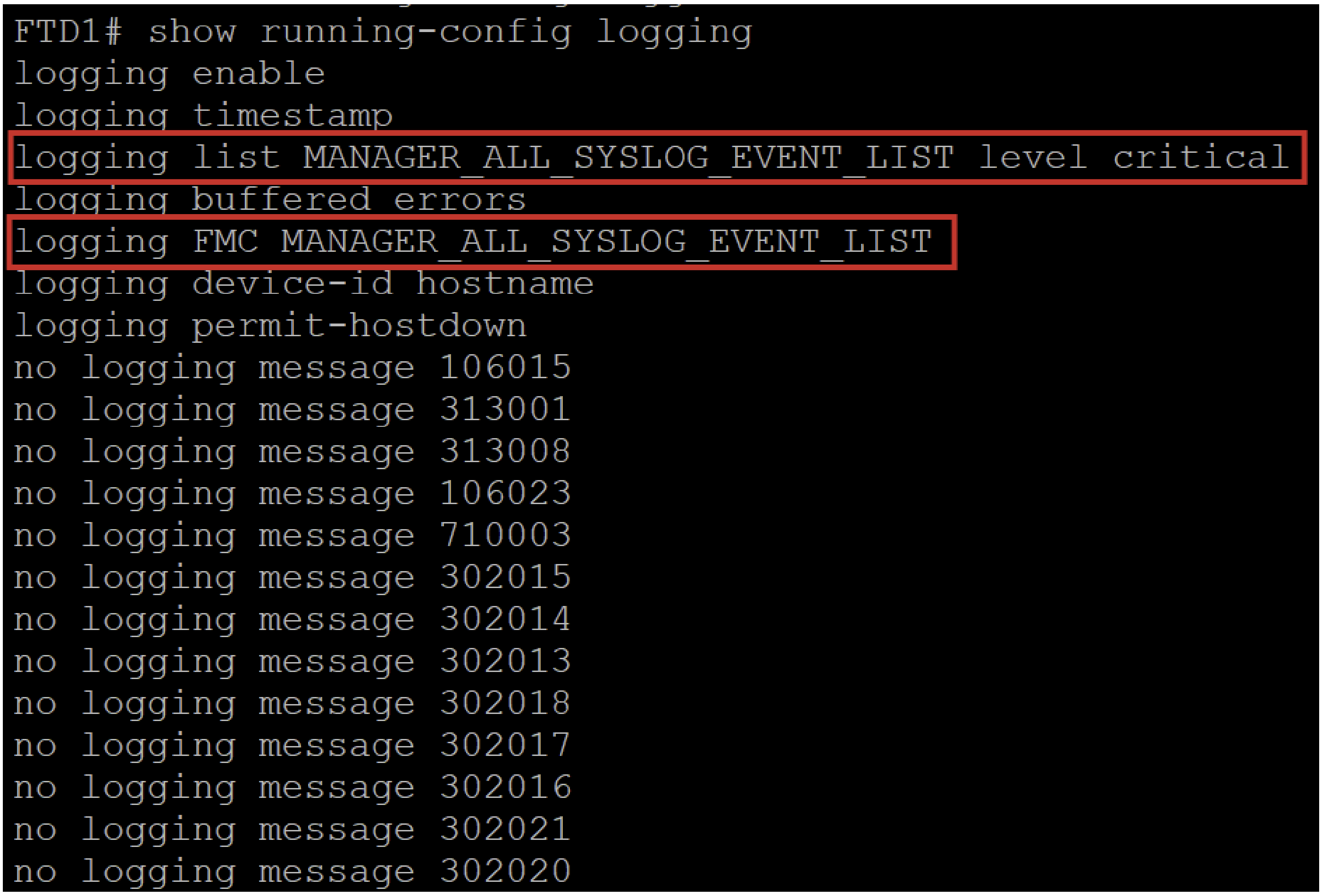
2025-01-15 15:33:44 IST – 2025-01-16 16:49:44 IST · 1d 1h

Time	Event Type	Source IP	Device	Domain	Message	Message Class
2025-01-16 16:40:48	Connection	198.51.100.111	FTD1	Global		
2025-01-16 16:39:32	Connection	198.51.100.145	FTD1	Global		
2025-01-16 16:37:38	Connection	198.51.100.39	FTD1	Global		
2025-01-16 16:36:28	Connection	203.0.113.75	FTD1	Global		
2025-01-16 16:35:22	Connection	203.0.113.153	FTD1	Global		
2025-01-16 16:33:10	Connection	198.51.100.49	FTD1	Global		
2025-01-16 16:32:10	Connection	198.51.100.95	FTD1	Global		
2025-01-16 16:31:15	Connection	192.0.2.25	FTD1	Global		
2025-01-15 19:59:43	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:59:27	Troubleshooting		FTD2	Global	(Secondary) Disabling f...	ha
2025-01-15 19:59:13	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:49:12	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:43:28	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
2025-01-15 19:42:58	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:42:54	Troubleshooting		FTD2	Global	(Secondary) No respon...	ha

Other Event Types

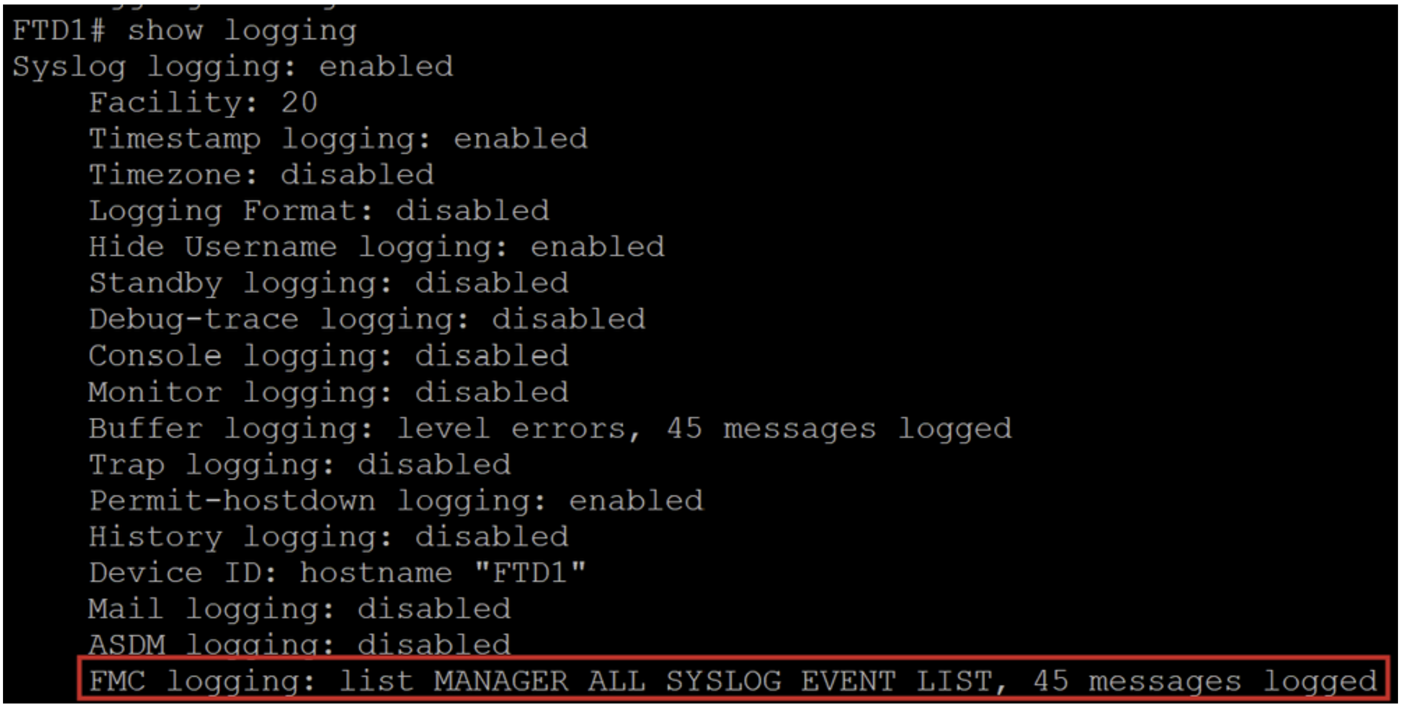
Verify the Configuration

Once the the configuration is done from the FMC GUI, it can be verified from the FTD CLI by running the commands **show running-config logging** and **show logging** in either CLISH or LINA mode.



```
FTD1# show running-config logging
logging enable
logging timestamp
logging list MANAGER_ALL_SYSLOG_EVENT_LIST level critical
logging buffered errors
logging FMC MANAGER_ALL_SYSLOG_EVENT_LIST
logging device-id hostname
logging permit-hostdown
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
```

FTD CLI Command



```
FTD1# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Timezone: disabled
    Logging Format: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level errors, 45 messages logged
    Trap logging: disabled
    Permit-hostdown logging: enabled
    History logging: disabled
    Device ID: hostname "FTD1"
    Mail logging: disabled
    ASDM logging: disabled
    FMC logging: list MANAGER ALL SYSLOG EVENT LIST, 45 messages logged
```

FTD CLI Command