# **Configure Devices to Send and View Troubleshooting Syslogs on FMC**

### Contents

ntroduction
rerequisites
Requirements
Components Used
eature Overview
Configure
<u>Verify the Configuration</u>

### 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.

Cisco Firewa	l Management Center Platform Settings	Q se	earch Deploy 🝼	• 🔮 💮 🛛 admin ~
Home				Object Management New Policy
Overview	Platform Settings	Device Type	Status	
III Analysis	FTD1_platform_settings	Threat Defense	Targeting 1 device(s) Up-to-date on all targeted devices	a <mark></mark> ⁄ī
Policies				
Devices				

Platform Settings Policy

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

~	FTD1_platform_set	ttings	Save Cancel
Home	Enter Description		
			Policy Assignments (1)
Overview		Logging Setup Logging Destinations Email Setup Event Lists Rate Limit Syslog Settings Syslog S	ervers
ad	ARP Inspection	Basic Logging Settings	
Analysis	Banner	Enable logging	
0	DNS	Enable logging on the failover standby unit	
Policies	External Authentication	Send syslogs in EMBLEM format	
	Fragment Settings	Send debug messages as syslogs	
=	HTTP Access	Memory Size of the Internal Buffer (bytes)	
Devices	ICMP Access	4096	
<b>*</b> =	NetFlow	(4096-52428800)	
Objects	SSH Access	Logging to Soours Firewall Management Contar	
	SMTP Server		
Integration	SNMP	Off  All Logs VPN Logs	
integration	SSL		
	Syslog		
	Timeouts	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).

22								Policy Assignments (1)
Overview		Logging Setup	Logging Destinations	Email Setup	Event Lists	Rate Limit	Syslog Settings	Syslog Servers
III Analysis Policies Devices	ARP Inspection Banner DNS External Authentication Fragment Settings HTTP Access ICMP Access	Basic Logging Enable logging Enable logging Send syslogs Send debug m Memory Size of th 4096	g Settings g on the failover standby u in EMBLEM format nessages as syslogs e Internal Buffer (bytes)	nit				
Objects	NetFlow SSH Access SMTP Server SNMP SSL Syslog Timeouts Time Synchronization	(4096-52428800) Logging to Se Off  A Logging Level 2 - critical 0 - emergencies 1 - alerts	cure Firewall Manae	gement Cent	er			
		2 - critical		Available	Interface Group	os C	Sele	cted Interface Groups

Available Logging Levels

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

21			Policy Assignments (1)
Overview		Logging Setup Logging Destinations Email Setup Event Lists Rate Limit Syslog Settings Syslog Servers	
and the	ARP Inspection	Basic Logging Settings	
Analysis	Banner		
	DNS	Enable logging on the failover standby unit	
Policies	External Authentication	Send syslogs in EMBLEM format	
	Fragment Settings	Send debug messages as syslogs	
=	HTTP Access	Memory Size of the Internal Buffer (bytes)	
Devices	ICMP Access	4096	
•	NetFlow	(4098-52428800)	
Objects	SSH Access		
	SMTP Server	Logging to secure Firewail Management Center	
÷	SNMP	Off All Logs OVPN Logs	
Integration	SSL	Logging Level	
	Syslog	3 - errors	
	Timeouts	0 - emergencies	
	Time Synchronization	1 - alerts	
	Time Zone	2 - critical Available Interface Groups C Selected Interface Groups	
	UCAPL/CC Compliance	3 - errors	
	Performance Profile	4 - warnings	
		5 - notifications	
		6 - informational	
		7 - debugging Add	
		·	

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**.

ဂျာဂျာဂ င၊sco	Firewall Manage Devices / Troubleshoo	ement Center t / Troubleshooting Logs		Q Search	Deploy	ලං 🤪 🐼 🧐	) admin ~
Home	9			Bookmark This	Page   Create Report   D 2025-0	Dashboard   View Bo 01-15 15:33:00 - 20	ookmarks   Search 25-01-16 16:49:00 Static
Overvie	No Search Con Table View	straints (Edit Search) r of Troubleshooting Logs	]				
II Analys	iis	] ↓ Time ×	Severity $\times$	Message ×	Message Class $ imes$	Username $\times$	Device $\times$
Policie	÷ [	) 2025-01-15 19:59:43	Alert	(Primary) No response from other firewall (reason code = 4).	ha		FTD1
1	+ -	) 2025-01-15 19:59:27	Alert	(Secondary) Disabling failover.	ha		FTD2
Devie	+ [	) 2025-01-15 19:59:13	Alert	(Primary) No response from other firewall (reason code = 3).	ha		FTD1
Device	÷ [	) 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
Object	ŧs ₩	) 2025-01-15 19:42:58	Alert	(Primary) No response from other firewall (reason code = 4).	ha		FTD1
<b>5</b> -	+ 🗆	2025-01-15 19:42:54	Alert	(Secondary) No response from other firewall (reason code = 4).	ha		FTD2
Integrat	ion ₹ □	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**.

Analysis	II Management Cente / Unified Events	r		Q Search		Deploy 💽 🔮	🐼 🕐 🛛 admin 🗸	~
Home	Events Troubleshootin	g						
Overview	Q Search	₩0 d 14 events				2025-01-16 15:33 2025-01-16 16:49	☆ ⑧ Refres	sh
ad	Time	Event Type	Action	Reason	Source IP	Destination IP	Source Po ICMP Type	
Analysis	> 2025-01-16 16:49:27	S Connection	Block		198.51.100.178	192.0.2.171	2906 / tcp	-
0	> 2025-01-16 16:48:37	S Connection	Block		198.51.100.134	192.0.2.171	9025 / tcp	
Policies	> 2025-01-16 16:47:17	S Connection	Allow		203.0.113.234	192.0.2.51	8902 / tcp	
	> 2025-01-16 16:46:17	S Connection	Allow		203.0.113.149	198.51.100.27	6789 / tcp	
Devices	> 2025-01-16 16:43:58	$\Leftrightarrow$ Connection	Block		192.0.2.214	203.0.113.139	8080 / tcp	
Devices	> 2025-01-16 16:43:25	S Connection	Block		192.0.2.214	198.51.100.71	8080 / tcp	
*=	> 2025-01-16 16:40:48	S Connection	Allow		198.51.100.111	203.0.113.66	8 (Echo Re	
Objects	> 2025-01-16 16:39:32	$\Leftrightarrow$ Connection	Allow		198.51.100.145	203.0.113.186	8 (Echo Re	
	> 2025-01-16 16:37:38	S Connection	Block		198.51.100.39	192.0.2.176	7413 / tcp	
Integration	> 2025-01-16 16:36:28	S Connection	Block		203.0.113.75	198.51.100.112	8421 / tcp	
	> 2025-01-16 16:35:22	$\Leftrightarrow$ Connection	Allow		203.0.113.153	192.0.2.132	9876 / tcp	
	> 2025-01-16 16:33:10	S Connection	Block		198.51.100.49	192.0.2.63	3692 / tcp	
	> 2025-01-16 16:32:10	S Connection	Allow		198.51.100.95	203.0.113.99	8 (Echo Re	
	> 2025-01-16 16:31:15	$\Leftrightarrow$ 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**.

းပြားပြား cisco	Firewall M Analysis / Unif	anagement Center ied Events			Q Search		Deploy 🕐 O 🧬	& @	admin 🗸
Home	Ev	ents Troubleshooting							
Overvier	Q * 35	Event Type Troubleshoo	ting +				2025-01-15 15:33 2025-01-16 16:45	844 IST 1d 1h	Refresh Go Live
aut		Time	Event Type	Source IP	Device	Domain	Message	Message C	las: 🔳
Analysi	s >	2025-01-15 19:59:43	* Troubleshooting		FTD1	Global	(Primary) No response	f ha	1
0	>	2025-01-15 19:59:27	* Troubleshooting		FTD2	Global	(Secondary) Disabling	f ha	
Policies	•	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	
Devices	>	2025-01-15 19:43:28	* Troubleshooting		FTD2	Global	(Secondary) Switching	t ha	
Devices	, ,	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	n ha	
Objects	5 <b>&gt;</b>	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	n ha	
Integrati	on >	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.

cisco Analys	wall Management ( sis / Unified Events	Center		Q se	earch	Deploy 🔇 O 🌘	🖗 🕲	admin 🗸
Home	Events Troubles	shooting						
	Q × Event Type		8	Refresh				
Overview	* 399 5 14 5	👽 🗅 🗼 🗄 413 e	vents			2025-01-15 2025-01-16	15:33:44 IST 1d 1h 16:49:44 IST 1d 1h	• Go Live
ald	Time	Event Type	Source IP	Device	Domain	Message	Message	Clas: 🔟
Analysis	> 2025-01-16 16:	40:48	198.51.100.111	FTD1	Global			:
Ø	> 2025-01-16 16:	39:32 5 Connection	198.51.100.145	FTD1	Global			1
Policies	> 2025-01-16 16:	37:38 🔄 Connection	198.51.100.39	FTD1	Global			1
	> 2025-01-16 16:	36:28 🔄 Connection	203.0.113.75	FTD1	Global			1
Devices	> 2025-01-16 16:	35:22 🔄 Connection	203.0.113.153	FTD1	Global			1
	> 2025-01-16 16:	33:10 5 Connection	198.51.100.49	FTD1	Global			1
≜	> 2025-01-16 16:	32:10 S Connection	198.51.100.95	FTD1	Global			1
Objects	> 2025-01-16 16:	31:15 S Connection	192.0.2.25	FTD1	Global			+
	> 2025-01-15 19:	59:43 🛠 Troubleshooting		FTD1	Global	(Primary) No respo	onse f ha	
Integration	> 2025-01-15 19:	59:27 🛠 Troubleshooting		FTD2	Global	(Secondary) Disat	oling f ha	
	> 2025-01-15 19:	59:13 😤 Troubleshooting		FTD1	Global	(Primary) No respo	onse f ha	
	> 2025-01-15 19:	49:12 * Troubleshooting		FTD1	Global	(Primary) No respo	onse f ha	
	> 2025-01-15 19:	43:28 🎌 Troubleshooting		FTD2	Global	(Secondary) Swite	hing t ha	
	> 2025-01-15 19:	42:58 🎋 Troubleshooting		FTD1	Global	(Primary) No respo	onse f ha	
	· 2025 01 15 10-	AD-EA SE Travelashaating		CTD0	Clobal	(Conondana) No re	anon 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