

# Configuración de dispositivos para enviar y ver los registros del sistema de resolución de problemas en FMC

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Descripción general de características](#)

[Configurar](#)

[Verifique la Configuración](#)

---

## Introducción

Este documento describe cómo configurar los dispositivos administrados para enviar mensajes de syslog de diagnóstico a FMC y verlos en el Visor de Eventos Unificado.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Mensajes de Syslog
- Centro de administración Firepower (FMC)
- Firepower Threat Defense (FTD)

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Este documento se aplica a todas las plataformas Firepower.
- Secure Firewall Threat Defence Virtual (FTD), que ejecuta la versión de software 7.6.0
- Secure Firewall Management Center Virtual (FMC), que ejecuta la versión de software 7.6.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

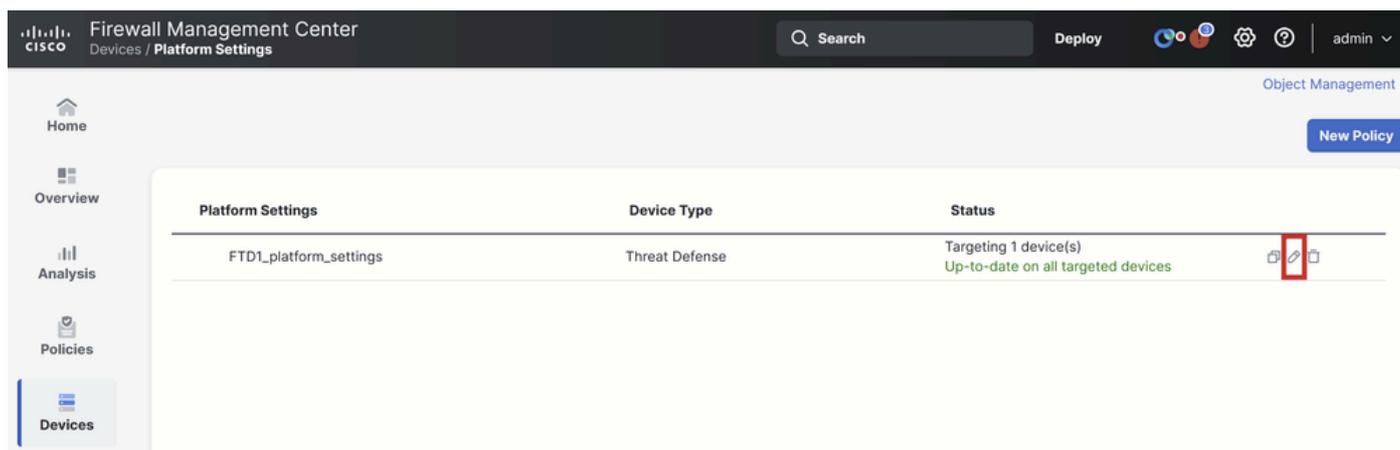
## Descripción general de características

En Secure Firewall 7.6, se agrega un nuevo tipo de evento de Troubleshooting en la tabla del visor de eventos de Unified. La configuración de la plataforma syslog logging configuration se ha ampliado y admite el envío de mensajes de syslog de diagnóstico generados por LINA al FMC en lugar de solamente registros de VPN. Esta función se puede configurar en cualquier FTD que ejecute una versión de software compatible con FMC 7.6.0. cdFMC no es compatible porque cdFMC no tiene herramientas de análisis.

- La opción Todos los registros está limitada a los niveles de registro crítico, de alerta y de emergencia debido al volumen de eventos.
- Estos registros de solución de problemas muestran cualquier registro del sistema enviado desde el dispositivo al FMC (VPN u otro).
- Los registros de solución de problemas se envían al FMC y son visibles en la vista de eventos unificada y en Dispositivos > Solución de problemas > Registros de solución de problemas.

## Configurar

Navegue hasta FMC Devices > Platform Settings y haga clic en el icono Edit en la esquina superior derecha de la política.



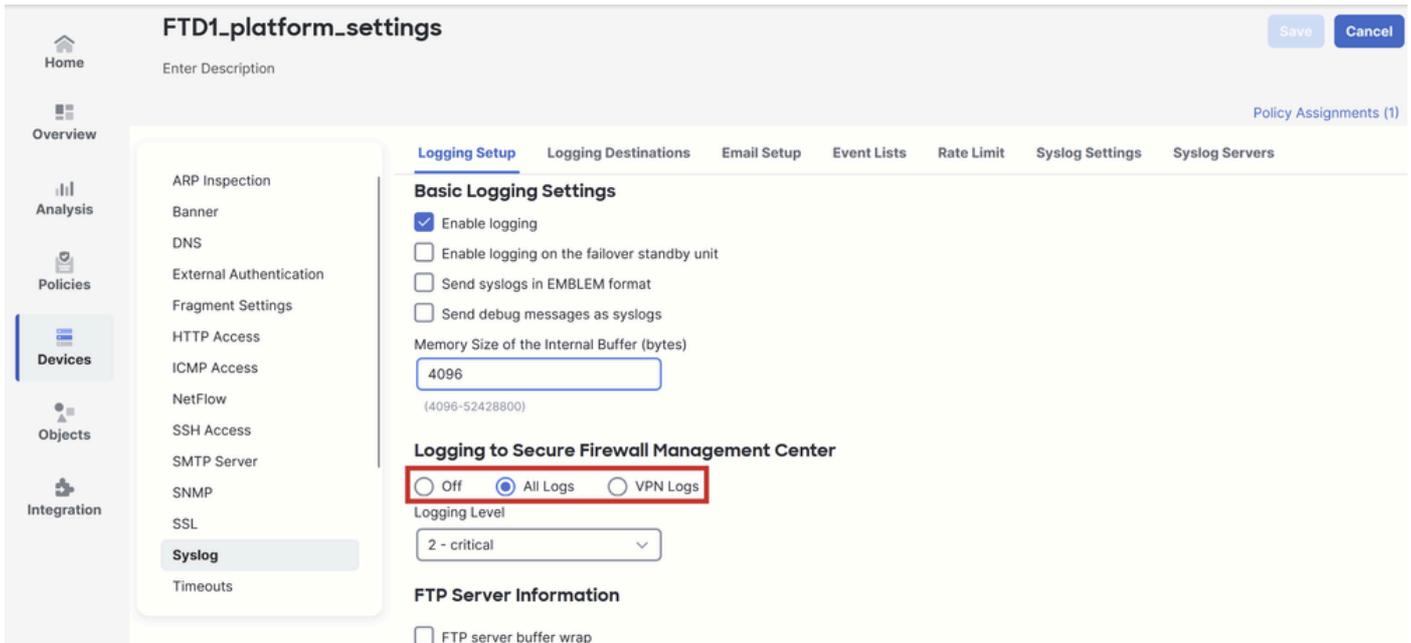
The screenshot shows the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes the Cisco logo, the text "Firewall Management Center" and "Devices / Platform Settings", a search bar, a "Deploy" button, and user information "admin". The main content area displays a table of Platform Settings. The table has three columns: "Platform Settings", "Device Type", and "Status". A single row is visible with the following data:

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

On the right side of the row, there are three icons: a copy icon, an edit icon (highlighted with a red box), and a delete icon. A "New Policy" button is located in the top right corner of the table area.

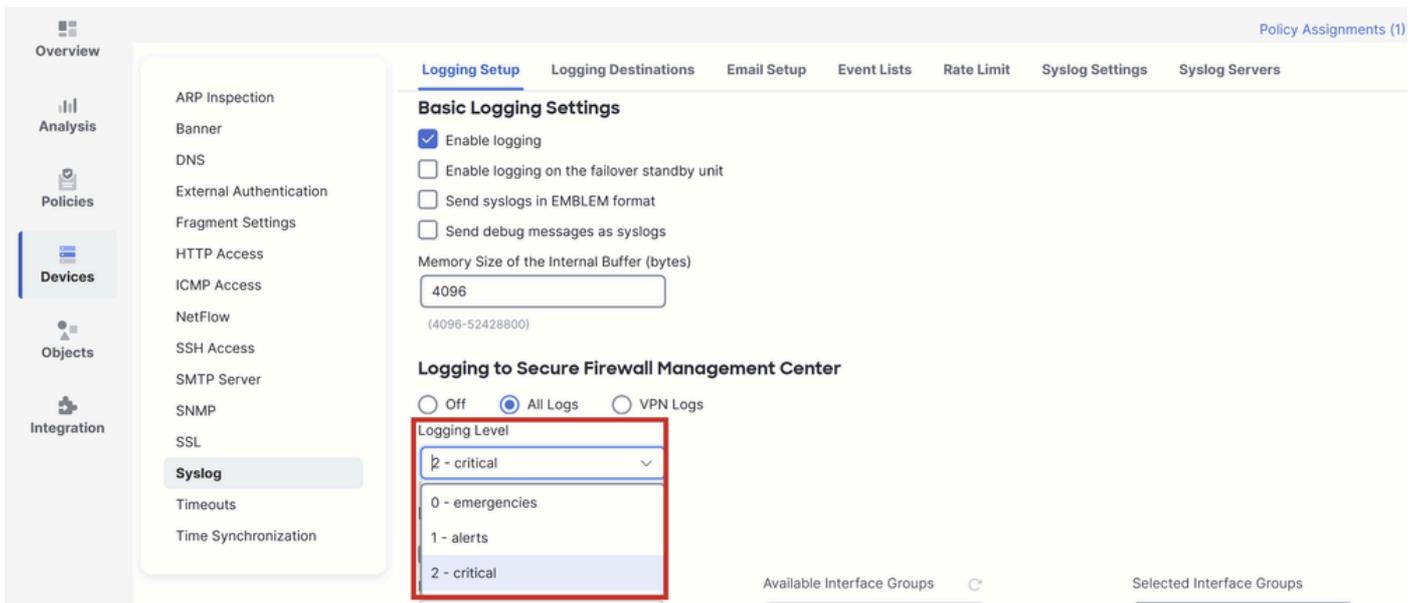
Directiva de configuración de plataforma

Vaya a Syslog > Configuración de registro. Puede ver tres opciones en Registro en Secure Firewall Management Center.



Tres opciones de registro

Si selecciona All Logs, puede seleccionar cualquiera de los tres niveles de registro disponibles: emergencias, alertas y mensajes críticos y enviar todos los mensajes de syslog de diagnóstico a FMC (incluida VPN).



Niveles de registro disponibles

Si elige VPN Logs, todos los niveles de registro están disponibles y se puede seleccionar uno de ellos.

Policy Assignments (1)

Overview

Analysis

Policies

**Devices**

Objects

Integration

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

**Syslog**

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Performance Profile

Logging Setup | Logging Destinations | Email Setup | Event Lists | Rate Limit | Syslog Settings | Syslog Servers

### 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

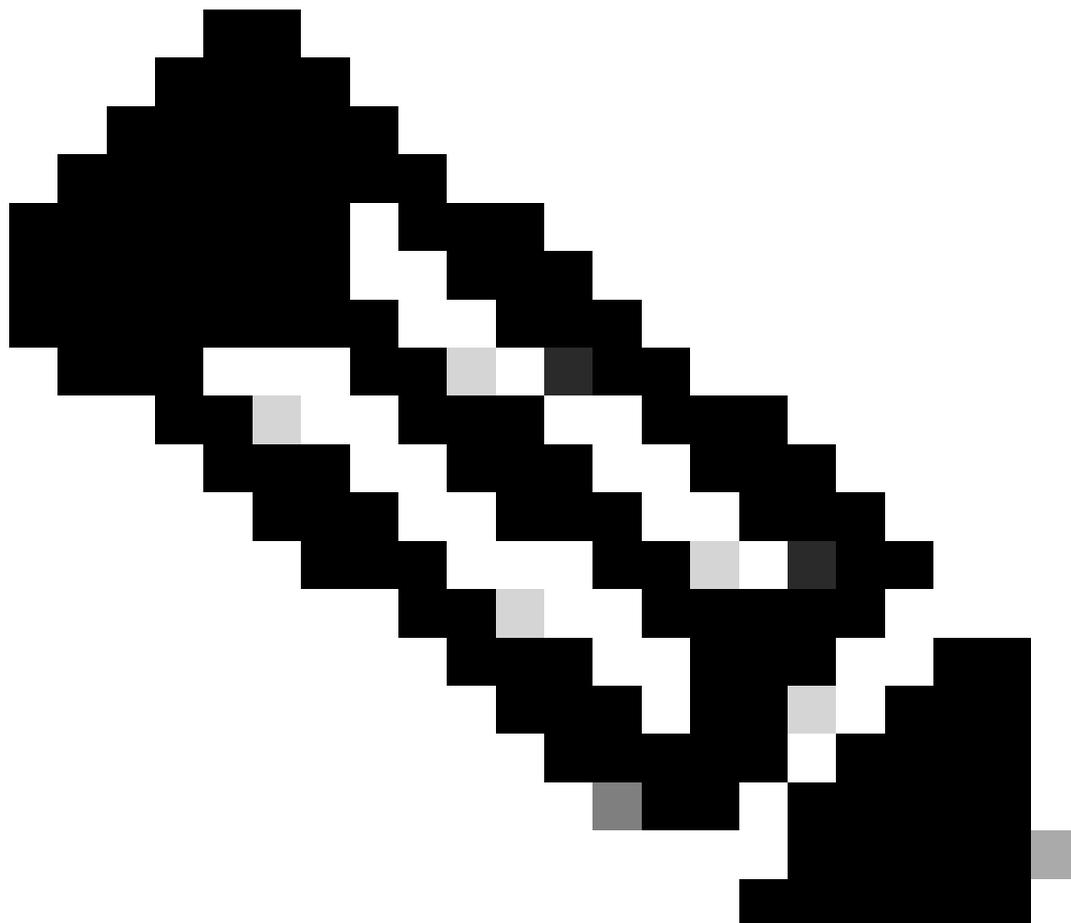
- 3 - errors
- 0 - emergencies
- 1 - alerts
- 2 - critical
- 3 - errors
- 4 - warnings
- 5 - notifications
- 6 - informational
- 7 - debugging

Available Interface Groups

Selected Interface Groups

Add

Niveles de registro disponibles



Nota: Al configurar un dispositivo con VPN de sitio a sitio o de acceso remoto, se habilita

automáticamente el envío de registros del sistema VPN al centro de administración de forma predeterminada. Puede cambiarlo a Todos los registros para enviar todos los registros del sistema además de los registros de VPN a FMC.

Se puede acceder a estos registros desde **Devices > Troubleshoot > Troubleshooting Logs**.

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes the Cisco logo, the title "Firewall Management Center", and the breadcrumb "Devices / Troubleshoot / Troubleshooting Logs". A search bar and a "Deploy" button are also visible. The left sidebar contains navigation options: Home, Overview, Analysis, Policies, Devices (highlighted), Objects, and Integration. The main content area displays "Table View of Troubleshooting Logs" with a table of log entries. The table has columns for Time, Severity, Message, Message Class, Username, and Device. The log entries show various alerts from devices FTD1 and FTD2, including messages like "No response from other firewall" and "Switching to OK".

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

Vista de tabla de registros de solución de problemas

Ahora hay disponible una nueva ficha de vista de solución de problemas en la página Visor de sucesos de Unified. Para ver estos eventos, vaya a **Análisis > Eventos unificados > Solución de problemas**.

Firewall Management Center Analysis / Unified Events

Search Deploy admin

Events Troubleshooting

Search... Refresh

14 0 0 0 14 events 2025-01-16 15:33:44 IST 1h 16m Go Live

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	

Vista de solución de problemas

Un nuevo tipo de evento es visible dentro de la tabla una vez que cambie a esta ficha. No se puede agregar ni quitar de la vista como los demás tipos, ya que es fundamental para la vista Solución de problemas.

Firewall Management Center Analysis / Unified Events

Search Deploy admin

Events Troubleshooting

Event Type Troubleshooting + Refresh

399 399 events 2025-01-15 15:33:44 IST 1d 1h Go Live

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

Tipo de evento de resolución de problemas

Aún se pueden agregar y quitar otros tipos de eventos de esta vista Solución de problemas. Esto permite ver los registros de diagnóstico junto con otros datos de eventos.

Firewall Management Center  
Analysis / Unified Events

Search Deploy admin

Events Troubleshooting

Event Type Troubleshooting Connection Intrusion + Refresh

399 14 0 413 events 2025-01-15 15:33:44 IST 1d 1h Go Live

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 response f...	ha

Otros tipos de eventos

## Verifique la Configuración

Una vez que la configuración se realiza desde la GUI de FMC, se puede verificar desde la CLI de FTD ejecutando los comandos `show running-config logging` y `show logging` en el modo CLISH o LINA.

```
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
```

Comando CLI de FTD

```
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
```

Comando CLI de FTD

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).