

Apparaten configureren voor verzenden en weergeven van probleemoplossingslogs op FMC

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Overzicht van functies](#)

[Configureren](#)

[De configuratie verifiëren](#)

Inleiding

Dit document beschrijft hoe u beheerde apparaten moet configureren om diagnostische syslogberichten naar FMC te verzenden en deze in het Unified Event Viewer te bekijken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

Syslog Berichten

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Dit document is van toepassing op alle FirePOWER-platforms.
- Secure Firewall Threat Defense Virtual (FTD), versie 7.6.0
- Secure Firewall Management Center Virtual (FMC) met softwareversie 7.6.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht van functies

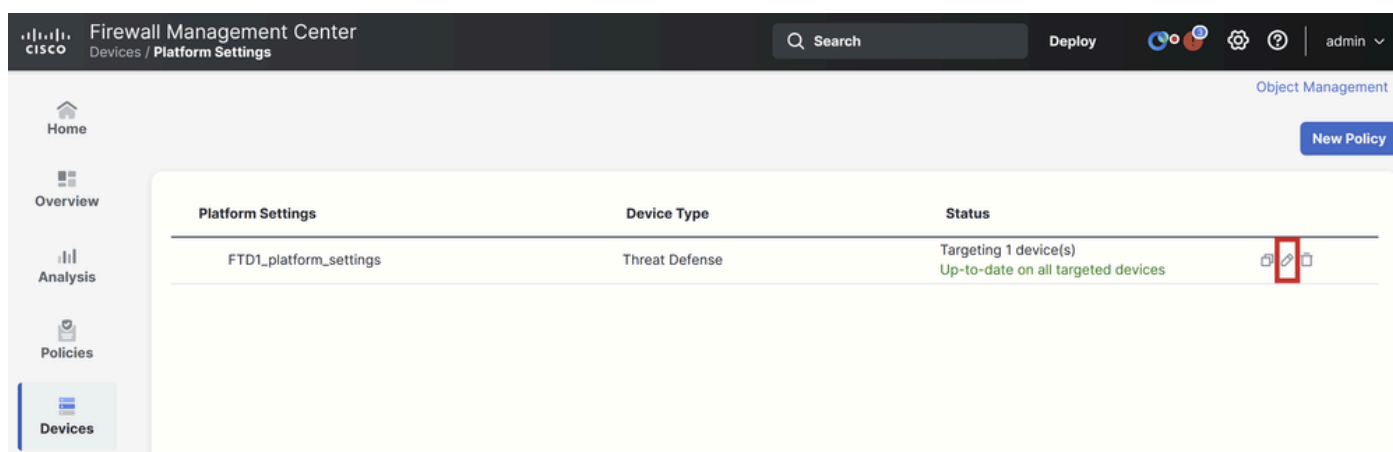
In Secure Firewall 7.6 wordt een nieuw type probleemoplossing toegevoegd in de tabel in het

Unified Event Viewer. De configuratie van de platforminstellingen voor syslog-logboekregistratie is uitgebreid en ondersteunt het verzenden van LINA-gegenereerde diagnostische syslog-berichten naar het VCC in plaats van alleen VPN-logbestanden. Deze optie kan worden geconfigureerd op elke FTD met een softwareversie die compatibel is met FMC 7.6.0. CDFMC wordt niet ondersteund omdat cdFMC geen analysetools heeft.

- De optie Alle logbestanden is beperkt tot nood-, waarschuwings- en kritische logniveaus vanwege het volume van de gebeurtenis.
- Deze logbestanden voor probleemoplossing tonen alle syslog die van het apparaat naar het VCC (VPN of andere) wordt verzonden.
- De logbestanden voor probleemoplossing worden doorgestuurd naar het VCC en zijn zichtbaar in de Unified Event View en onder Apparaten > Probleemoplossing > Logbestanden voor probleemoplossing.

Configureren

Navigeer naar FMC Devices > Platform Settings en klik op Edit icon in de rechterbovenhoek van het beleid.



The screenshot shows the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes the Cisco logo, 'Firewall Management Center', and 'Devices / Platform Settings'. A search bar and a 'Deploy' button are also visible. The main content area displays a table of Platform Settings. The table has three columns: Platform Settings, Device Type, and Status. The first row shows 'FTD1_platform_settings' under Platform Settings, 'Threat Defense' under Device Type, and 'Targeting 1 device(s) Up-to-date on all targeted devices' under Status. An edit icon (pencil) is highlighted with a red box in the rightmost column of the first row.

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

Beleid inzake platforminstellingen

Ga naar Syslog > Logging instellen. U kunt drie opties zien onder Vastlegging naar Secure Firewall Management Center.

The screenshot shows the 'FTD1_platform_settings' interface. On the left is a navigation menu with categories: Home, Overview, Analysis, Policies, Devices (selected), Objects, and Integration. The 'Syslog' option is highlighted in the left menu. The main content area has tabs for 'Logging Setup', 'Logging Destinations', 'Email Setup', 'Event Lists', 'Rate Limit', 'Syslog Settings', and 'Syslog Servers'. Under 'Logging Setup', there are sections for 'Basic Logging Settings' (with checkboxes for 'Enable logging', 'Enable logging on the failover standby unit', 'Send syslogs in EMBLEM format', and 'Send debug messages as syslogs'), 'Memory Size of the Internal Buffer (bytes)' (set to 4096), and 'Logging to Secure Firewall Management Center' (with radio buttons for 'Off', 'All Logs', and 'VPN Logs', where 'All Logs' is selected). Below this is a 'Logging Level' dropdown menu set to '2 - critical'. At the bottom, there is a section for 'FTP Server Information' with a checkbox for 'FTP server buffer wrap'.

Drie vastlegging-opties

Als u Alle logbestanden kiest, kunt u een van de drie beschikbare registratieniveaus selecteren: noodgevallen, waarschuwingen en kritisch en verstuur alle diagnostische syslogberichten naar het VCC (inclusief VPN).

This screenshot is similar to the first one but shows the 'Logging Level' dropdown menu expanded. The dropdown is highlighted with a red box and lists four options: '2 - critical' (the currently selected option), '0 - emergencies', '1 - alerts', and '2 - critical'. The rest of the interface, including the 'All Logs' radio button, remains the same as in the previous screenshot.

Beschikbare registratieniveaus

Als u VPN Logs kiest, zijn alle registratieniveaus beschikbaar en kan één daarvan worden geselecteerd.

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

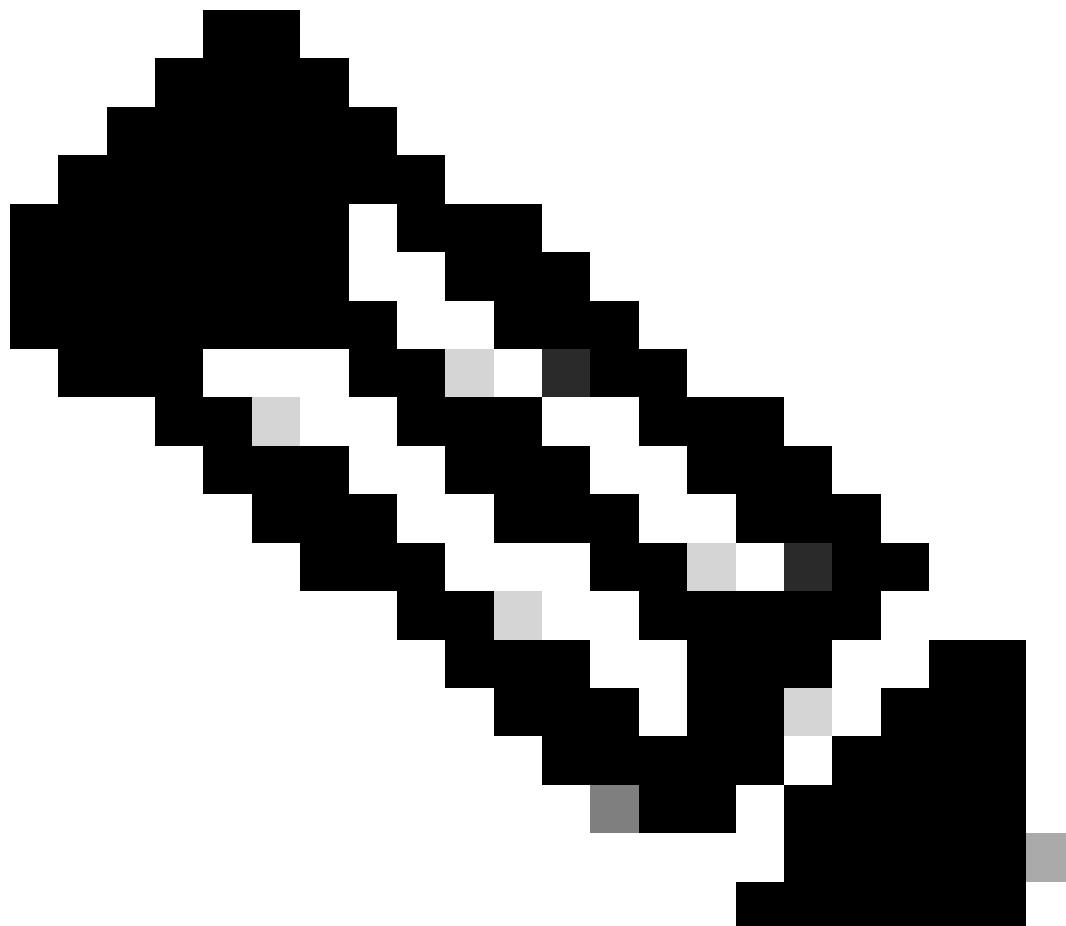
- 0 - emergencies
- 1 - alerts
- 2 - critical
- 3 - errors
- 4 - warnings
- 5 - notifications
- 6 - informational
- 7 - debugging

Available Interface Groups

Selected Interface Groups

Add

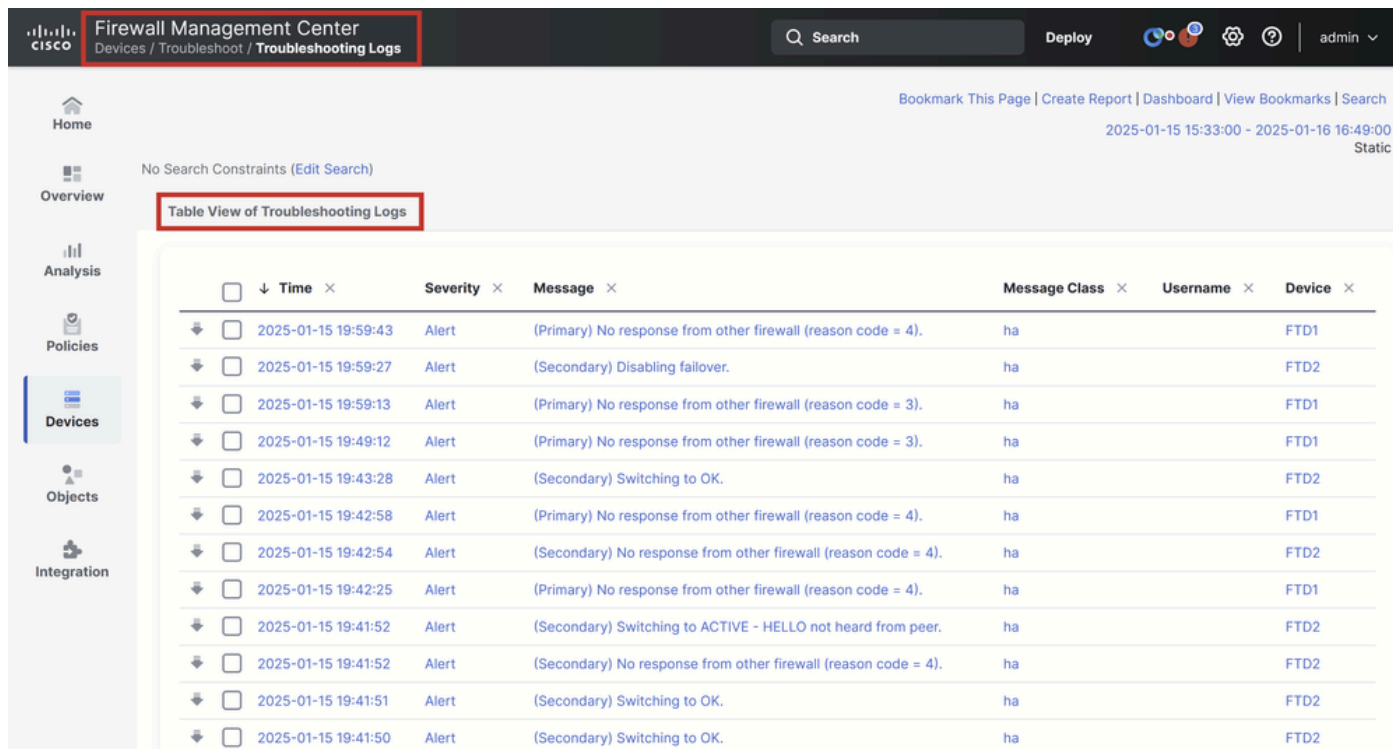
Beschikbare registratieniveaus



Opmerking: Wanneer u een apparaat configureert met site-to-site of externe toegang via

VPN, maakt het automatisch het verzenden van VPN-systemen naar het beheercentrum standaard mogelijk. U kunt deze wijzigen in All Logs om alle syslogs behalve VPN-logs naar FMC te sturen.

Deze logbestanden kunnen worden benaderd via Apparaten > Probleemoplossing > Logbestanden voor probleemoplossing.



The screenshot shows the Cisco Firewall Management Center 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 about firewall responses and failovers.

<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

Tabelweergave van logbestanden voor probleemoplossing

Er is nu een nieuw tabblad Problemen oplossen beschikbaar op de pagina Unified Event Viewer. Om deze gebeurtenissen te bekijken, navigeer naar Analyse > Unified Events > Problemen oplossen.

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

Weergave voor probleemoplossing

Er verschijnt een nieuw type gebeurtenis in de tabel zodra u naar dit tabblad switch. Het kan niet zoals de andere typen uit de weergave worden toegevoegd of verwijderd, omdat het van centraal belang is voor de weergave Problemen oplossen.

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

Type probleemoplossing

Er kunnen nog andere soorten gebeurtenissen worden toegevoegd en verwijderd uit de weergave Problemen oplossen. Dit stelt u in staat om diagnostische logboeken naast andere gebeurtenisgegevens te bekijken.

Firewall Management Center
Analysis / Unified Events

Search Deploy admin

Events Troubleshooting

Event Type Troubleshooting Connection Intrusion

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

Andere soorten gebeurtenissen

De configuratie verifiëren

Zodra de configuratie is uitgevoerd vanuit de FMC GUI, kan deze worden geverifieerd vanuit de FTD CLI door de opdrachten show in werking stellen-config vastlegging en logboekregistratie in CLISH of LINA modus tonen.

```
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-opdracht

```
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-opdracht

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.