

Configurare i dispositivi per l'invio e la visualizzazione dei syslog di risoluzione dei problemi in FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Panoramica delle funzionalità](#)

[Configurazione](#)

[Verifica della configurazione](#)

Introduzione

In questo documento viene descritto come configurare i dispositivi gestiti in modo che inviino messaggi di syslog di diagnostica a FMC e li visualizzino nel Visualizzatore eventi unificato.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Questo documento è valido per tutte le piattaforme Firepower.
- Secure Firewall Threat Defense Virtual (FTD) con software versione 7.6.0
- Secure Firewall Management Center Virtual (FMC) con software versione 7.6.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

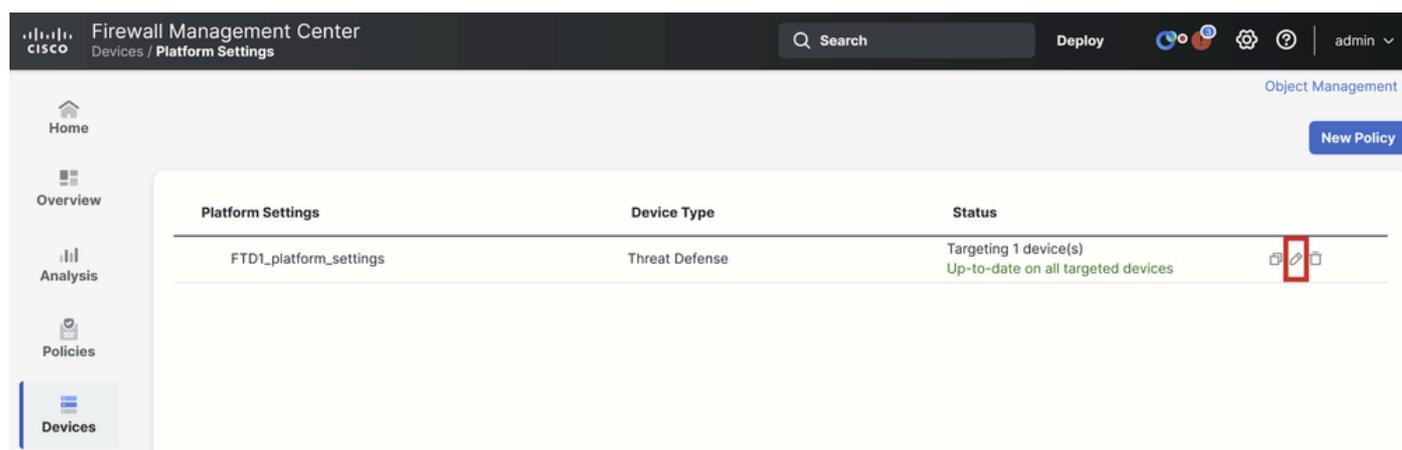
Panoramica delle funzionalità

In Secure Firewall 7.6, nella tabella del Visualizzatore eventi unificato viene aggiunto un nuovo tipo di evento Risoluzione dei problemi. La configurazione di registrazione syslog delle impostazioni della piattaforma è stata estesa e supporta l'invio di messaggi syslog di diagnostica generati da LINA al FMC anziché ai soli log VPN. Questa funzionalità può essere configurata su qualsiasi FTD che esegue una versione software compatibile con FMC 7.6.0. cdFMC non è supportato perché non dispone di strumenti di analisi.

- L'opzione Tutti i registri è limitata ai livelli di registro di emergenza, di avviso e critico a causa del volume degli eventi.
- Nei log di risoluzione dei problemi vengono visualizzati tutti i syslog inviati dal dispositivo al FMC (VPN o altro).
- I registri di risoluzione dei problemi vengono inviati al FMC e sono visibili nella Vista eventi unificata e in Dispositivi > Risoluzione dei problemi > Registri di risoluzione dei problemi.

Configurazione

Passare a Dispositivi FMC > Impostazioni piattaforma e fare clic su Icona Modifica nell'angolo superiore destro del criterio.



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 / Platform Settings". A search bar and a "Deploy" button are also visible. The main content area displays a table with the following structure:

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

The "Edit" icon in the table is highlighted with a red box. A "New Policy" button is located in the top right corner of the main content area.

Criterio impostazioni piattaforma

Passare a Syslog > Impostazione registrazione. In Accesso a Centro gestione firewall protetto sono disponibili tre opzioni.

The screenshot shows the 'FTD1_platform_settings' interface. On the left is a navigation menu with categories: Home, Overview, Analysis, Policies, Devices (highlighted), Objects, and Integration. The 'Syslog' option is selected 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 'Enable logging' checked), 'Logging to Secure Firewall Management Center' (with 'All Logs' selected), and 'FTP Server Information'.

Tre opzioni di registrazione

Se si sceglie Tutti i registri, è possibile selezionare uno dei tre livelli di registrazione disponibili: emergenze, avvisi e messaggi critici e inviare tutti i messaggi di syslog diagnostici al FMC (VPN inclusa).

This screenshot shows the same 'Logging Setup' page as above, but with the 'Logging Level' dropdown menu expanded. The menu lists four options: '2 - critical' (the current selection), '0 - emergencies', '1 - alerts', and '2 - critical'. The 'All Logs' radio button is also selected under the 'Logging to Secure Firewall Management Center' section.

Livelli di registrazione disponibili

Se si sceglie Registri VPN, saranno disponibili tutti i livelli di registrazione e sarà possibile selezionarne uno.

Policy Assignments (1)

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

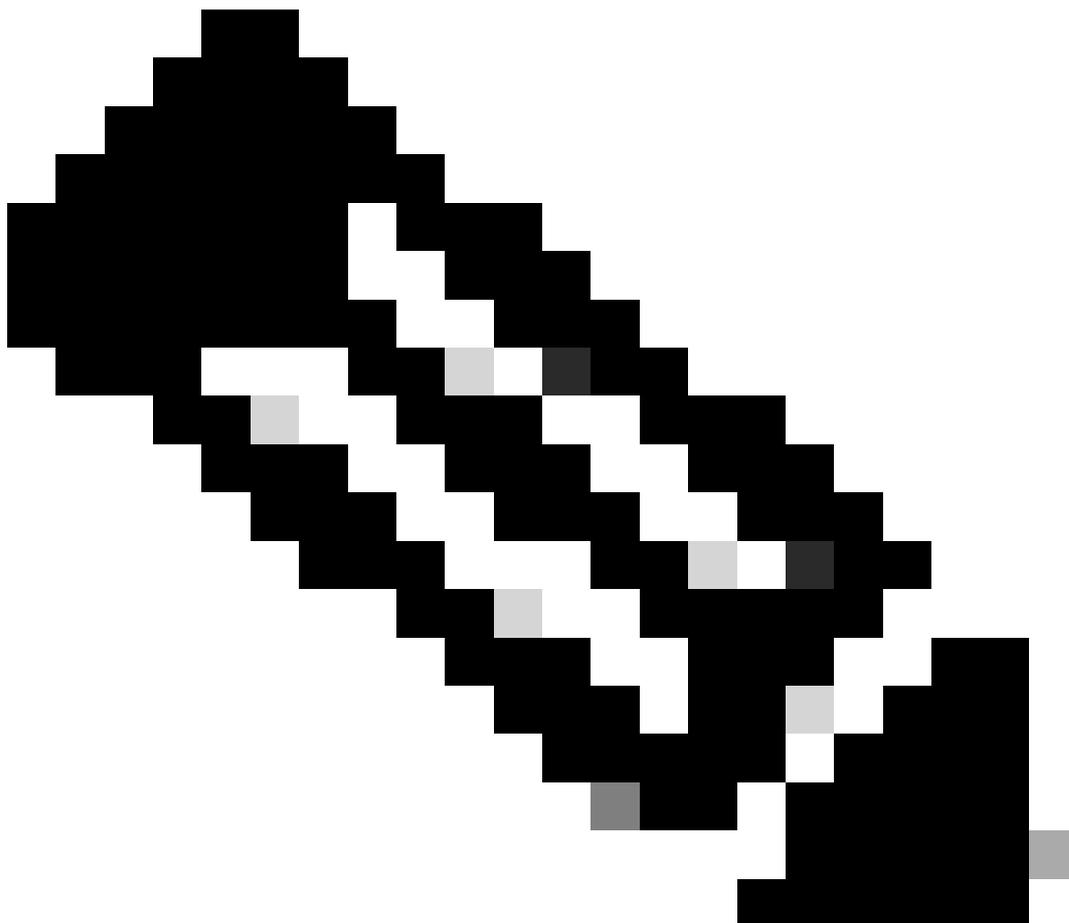
Logging Level: 3 - errors

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

Available Interface Groups: [Search] [Add]

Selected Interface Groups

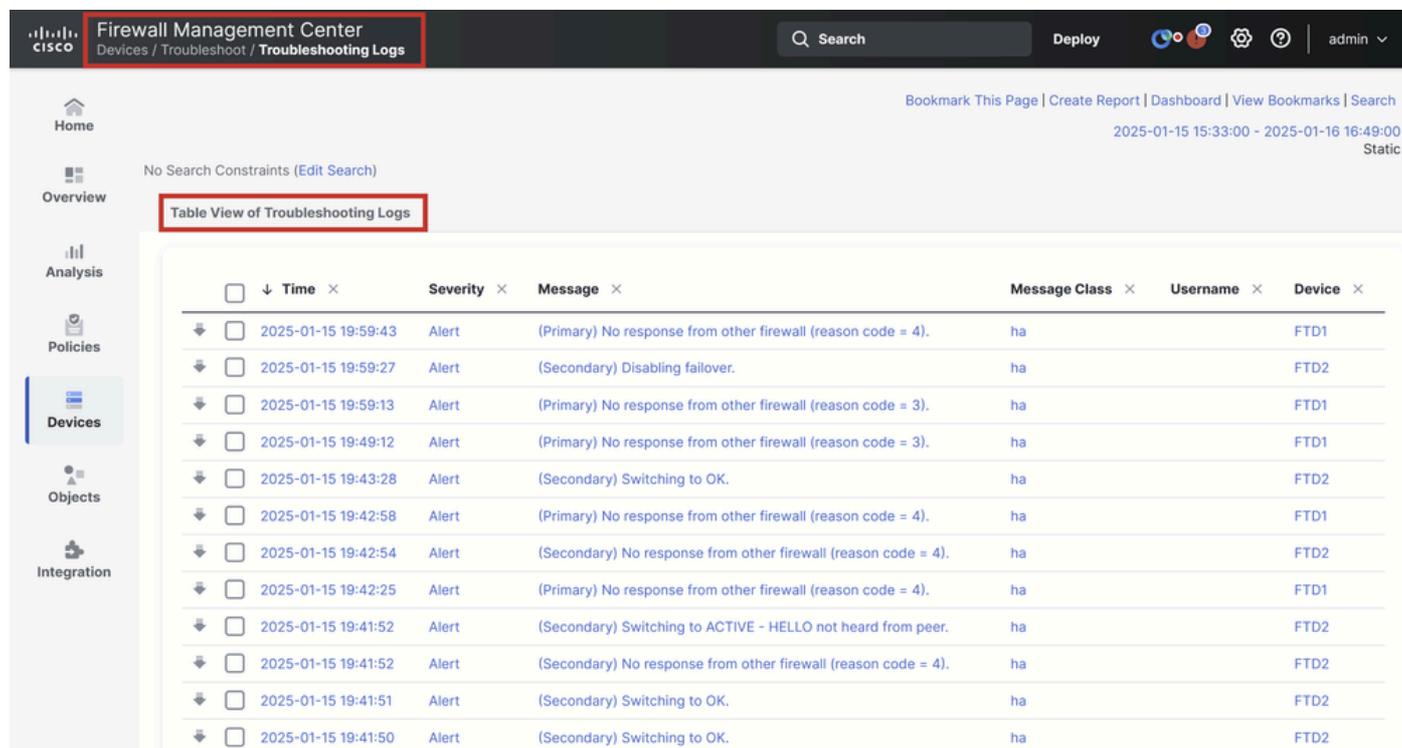
Livelli di registrazione disponibili



Nota: Quando si configura un dispositivo con una VPN da sito a sito o con accesso

remoto, per impostazione predefinita viene attivato automaticamente l'invio di syslog VPN al centro di gestione. È possibile modificarlo in Tutti i log per inviare tutti i syslog oltre ai log VPN a FMC.

È possibile accedere a questi log da Dispositivi > Risoluzione dei problemi > Log per la risoluzione dei problemi.



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 search filter set to "No Search Constraints (Edit Search)". The table lists log entries with columns for Time, Severity, Message, Message Class, Username, and Device.

<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

Visualizzazione per tabella dei log per la risoluzione dei problemi

Nella pagina Visualizzatore eventi unificato è ora disponibile una nuova scheda Visualizzazione Risoluzione problemi. Per visualizzare questi eventi, selezionare Analisi > Eventi unificati > Risoluzione dei problemi.

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

Visualizzazione Risoluzione problemi

Quando si passa a questa scheda, nella tabella viene visualizzato un nuovo tipo di evento. Non può essere aggiunto o rimosso dalla vista come gli altri tipi poiché è centrale nella vista Risoluzione problemi (Troubleshooting).

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 di evento risoluzione dei problemi

È comunque possibile aggiungere e rimuovere altri tipi di eventi da questa visualizzazione Risoluzione problemi. In questo modo è possibile visualizzare i log di diagnostica insieme ad altri dati degli eventi.

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
2025-01-15 19:42:54	Troubleshooting		FTD2	Global	(Secondary) No response f...	ha

Altri tipi di evento

Verifica della configurazione

Una volta eseguita la configurazione dalla GUI del FMC, è possibile verificarla dalla CLI del FTD eseguendo i comandi `show running-config log` e `show log` in modalità 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 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 FTD

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).