

Configurazione dei log sull'FTD tramite FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configura configurazione syslog globale](#)

[Configurazione registrazione](#)

[Elenchi di eventi](#)

[Syslog di limitazione della velocità](#)

[Impostazioni syslog](#)

[Configura registrazione locale](#)

[Configurare la registrazione esterna](#)

[Server Syslog Remoto](#)

[Configurazione e-mail per registrazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene spiegato come configurare la registrazione per FirePOWER Threat Defense (FTD) tramite Firepower Management Center (FMC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Tecnologia FirePOWER
- ASA (Adaptive Security Appliance)
- Protocollo Syslog

Componenti usati

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

- ASA Firepower Threat Defense Image per ASA (5506X/5506H-X/5506W-X, ASA 5508-X,

ASA 5516-X) con software versione 6.0.1 e successive

- ASA Firepower Threat Defense Image per ASA (5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) con software versione 6.0.1 e successive
- FMC versione 6.0.1 e successive

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.

Premesse

I registri di sistema FTD forniscono le informazioni necessarie per monitorare e risolvere i problemi relativi all'accessorio FTD.


I registri sono utili sia per la risoluzione dei problemi di routine che per la gestione degli incidenti. L'accessorio FTD supporta la registrazione locale ed esterna.

La registrazione locale consente di risolvere i problemi attivi. La registrazione esterna è un metodo di raccolta dei registri dall'accessorio FTD a un server Syslog esterno.

La registrazione su un server centrale consente l'aggregazione di registri e avvisi. La registrazione esterna può contribuire alla correlazione dei registri e alla gestione degli incidenti.

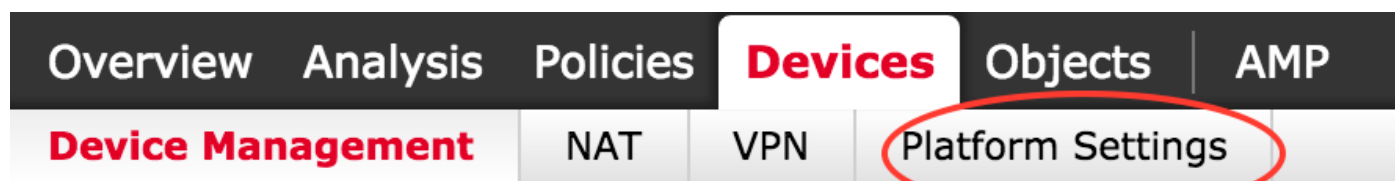
Per la registrazione locale, l'accessorio FTD supporta la console, l'opzione del buffer interno e la registrazione della sessione Secure Shell (SSH).

Per la registrazione esterna, l'accessorio FTD supporta il server Syslog esterno e il server Email Relay.

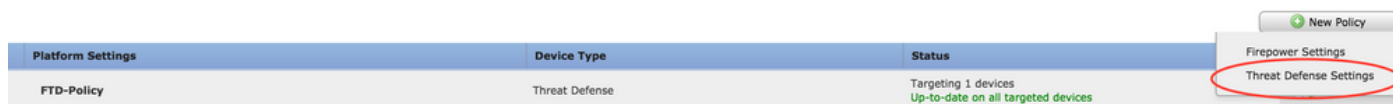
 Nota: se l'accessorio è attraversato da un volume di traffico elevato, prestare attenzione al tipo di registrazione, alla gravità o alla limitazione della velocità. Eseguire questa operazione per limitare il numero di registri ed evitare l'impatto sul firewall.

Configurazione

Tutte le configurazioni relative alla registrazione possono essere configurate quando si passa alla Platform Settings sotto la scheda Devices scheda. Scegli Devices > Platform Settings come mostrato nell'immagine.

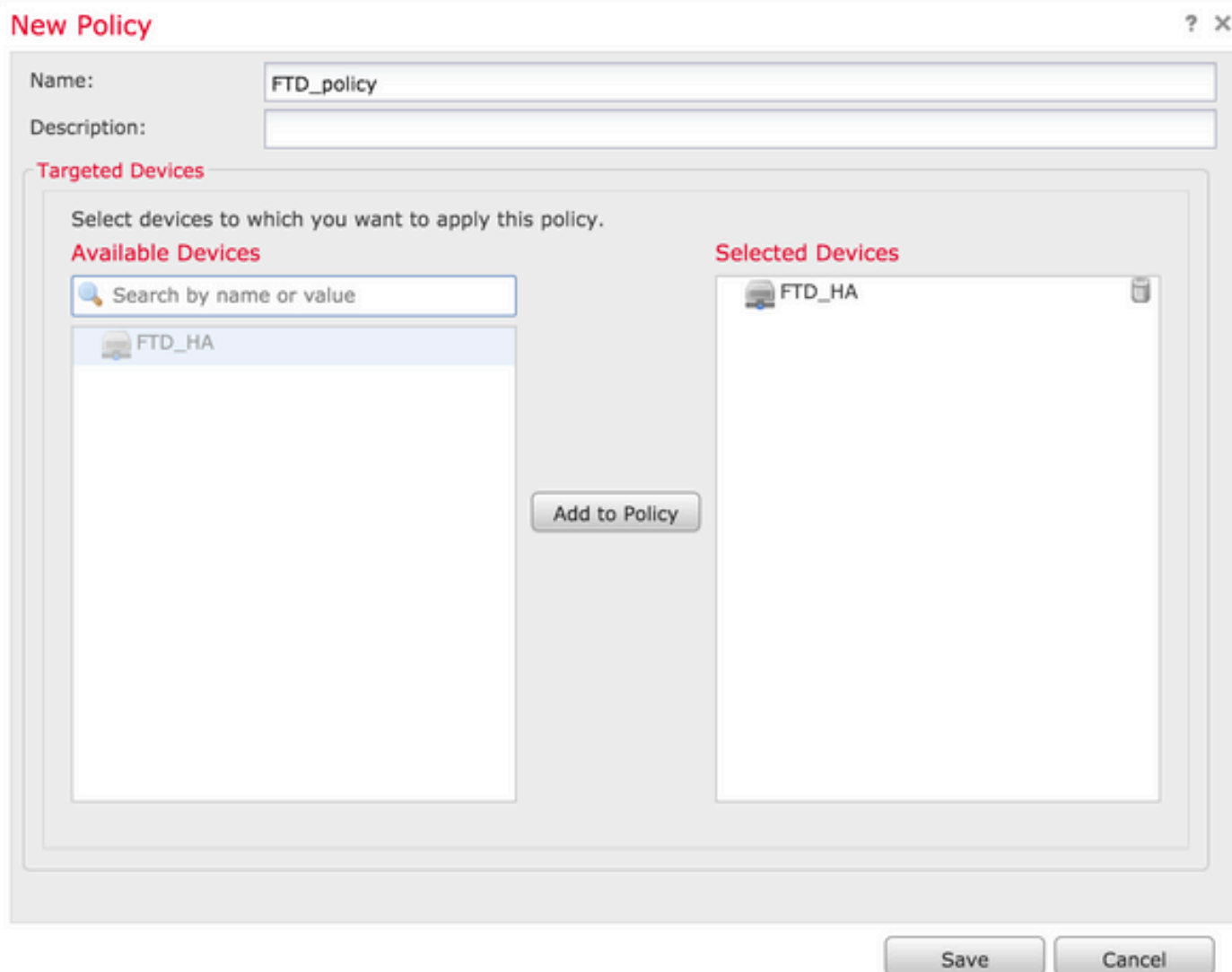


Fare clic sull'icona della matita per modificare il criterio esistente oppure fare clic su **New Policy** e quindi scegliere **Threat Defense Settings** per creare un nuovo criterio FTD, come mostrato nell'immagine.



Platform Settings	Device Type	Status
FTD-Policy	Threat Defense	Targeting 1 devices Up-to-date on all targeted devices

Scegliere l'accessorio FTD a cui applicare il criterio e fare clic su **save** come mostrato nell'immagine.



New Policy ? X

Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Search by name or value

FTD_HA

Selected Devices

FTD_HA

Add to Policy

Save Cancel

Configura configurazione syslog globale

Esistono alcune configurazioni applicabili per la registrazione locale ed esterna. In questa sezione vengono illustrati i parametri obbligatori e facoltativi che è possibile configurare per Syslog.

Configurazione registrazione

Le opzioni di impostazione della registrazione sono applicabili per la registrazione locale ed esterna. Per configurare l'impostazione di registrazione, scegliere **Devices > Platform Settings**.

Scegli **Syslog > Logging Setup**.

Configurazione di base della registrazione

- **Enable Logging**: controllare la **Enable Logging** per attivare la registrazione. Questa opzione è obbligatoria.
- **Enable Logging on the failover standby unit**: controllare la **Enable Logging on the failover standby unit** per configurare la registrazione sull'FTD in standby che fa parte di un cluster FTD ad alta disponibilità.
- **Send syslogs in EMBLEM format**: controllare la **Send syslogs in EMBLEM format** per abilitare il formato Syslog come EMBLEM per ogni destinazione. Il formato EMBLEM viene utilizzato principalmente per CiscoWorks Resource Manager Essentials (RME) Syslog Analyzer. Questo formato corrisponde al formato Syslog del software Cisco IOS prodotto dai router e dagli switch. È disponibile solo per i server Syslog UDP.
- **Send debug messages as syslogs**: controllare la **Send debug messages as syslogs** per inviare i log di debug come messaggi Syslog al server Syslog.
- **Memory size of the Internal Buffer**: immettere le dimensioni del buffer di memoria interno in cui FTD può salvare i dati di registro. Se viene raggiunto il limite del buffer, i dati del registro vengono ruotati.

Informazioni sul server FTP (facoltative)

Specificare i dettagli del server FTP se si desidera inviare i dati di registro al server FTP prima che sovrascriva il buffer interno.

- **FTP Server Buffer Wrap**: controllare la **FTP Server Buffer Wrap** per inviare i dati del log del buffer al server FTP.
- **IP Address**: immettere l'indirizzo IP del server FTP.
- **Username**: immettere il nome utente del server FTP.
- **Path**: immettere il percorso della directory del server FTP.
- **Password**: immettere la password del server FTP.
- **Confirm**: immettere di nuovo la stessa password.

Dimensioni Flash (Facoltativo)

Specificare le dimensioni del flash se si desidera salvare i dati del registro in modo che lampeggino una volta che il buffer interno è pieno.

- **Flash**: controllare la **Flash** per inviare i dati di registro al flash interno.
- **Maximum Flash to be used by Logging(KB)**: immettere la dimensione massima in KB della memoria flash utilizzabile per la registrazione.
- **Minimum free Space to be preserved(KB)**: immettere la dimensione minima in KB della memoria flash da mantenere.

Fare clic su **Save** per salvare l'impostazione della piattaforma. Scegliere il **Deploy** selezionare l'accessorio FTD a cui si desidera applicare le modifiche e fare clic su **Deploy** per avviare la distribuzione dell'impostazione della piattaforma.

Elenchi di eventi

L'opzione Configura elenchi eventi consente di creare/modificare un elenco di eventi e di specificare quali dati del registro includere nel filtro dell'elenco di eventi. Gli elenchi di eventi possono essere utilizzati quando si configurano i filtri di registrazione nelle destinazioni di registrazione.

Il sistema consente due opzioni per utilizzare la funzionalità degli elenchi di eventi personalizzati.

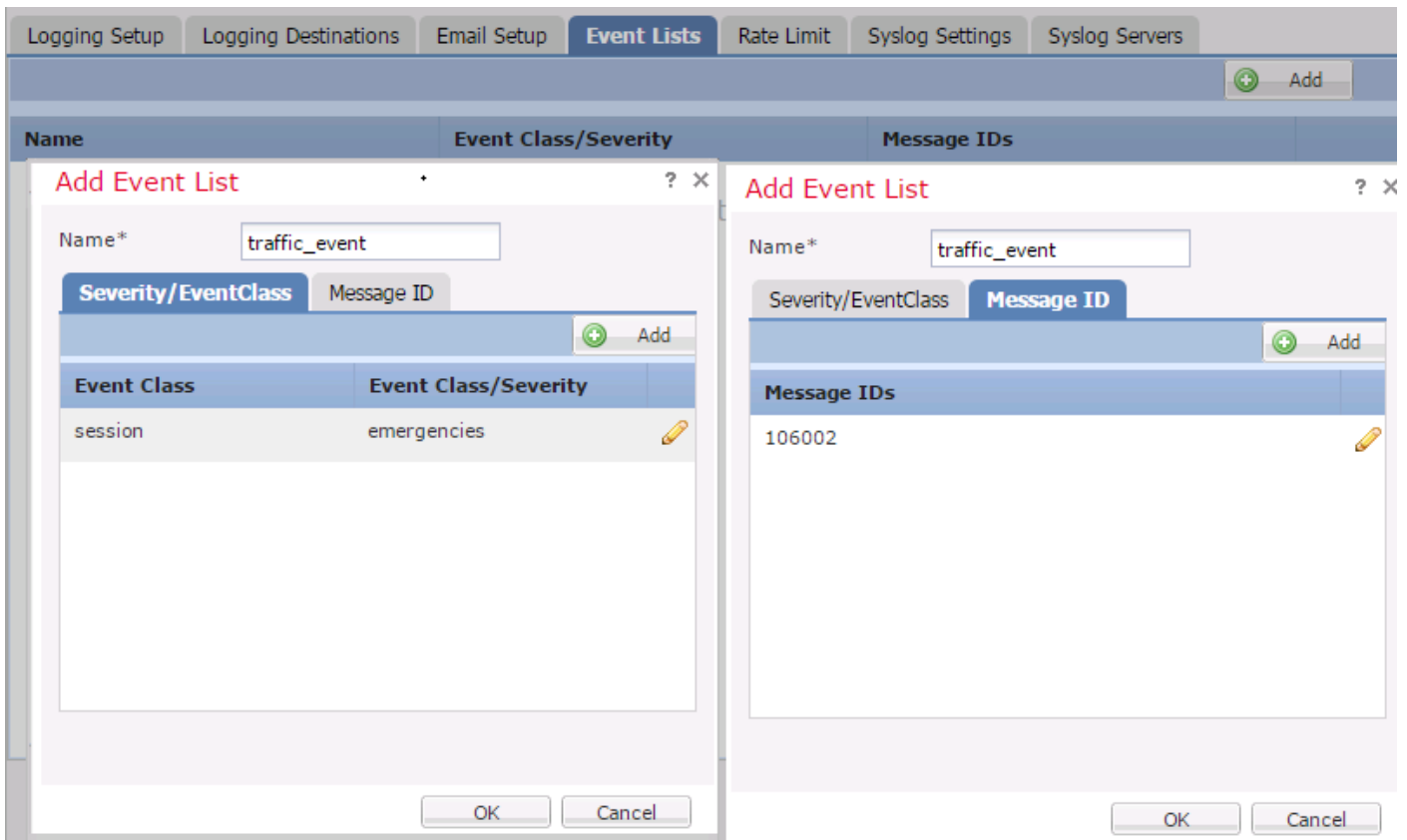
- Classe e gravità
- ID messaggio

Per configurare elenchi di eventi personalizzati, scegliere **Device > Platform Setting > Threat Defense Policy > Syslog > Event List** e fare clic su **Add**. Queste sono le opzioni:

- Name: immettere il nome dell'elenco di eventi.
- Severity/Event Class: nella sezione Classe di gravità/evento, fare clic su **Add**.
- Event Class: scegliere la classe di evento dall'elenco a discesa per il tipo di dati di registro desiderato. Una classe Event definisce un insieme di regole Syslog che rappresentano le stesse funzionalità.

Ad esempio, esiste una classe di evento per la sessione che include tutti i syslog relativi alla sessione.

- Syslog Severity: scegliere la severità dall'elenco a discesa per la classe di evento scelta. La gravità può variare da 0 (emergenza) a 7 (debug).
- Message ID: se si è interessati a dati di registro specifici relativi a un ID messaggio, fare clic su **Add** per applicare un filtro basato sull'ID del messaggio.
- Message IDs: specifica l'ID messaggio come formato singolo/intervallo.



Fare clic su **OK** per salvare la configurazione.

Fare clic su **Save** per salvare l'impostazione della piattaforma. Scegli di **Deploy**, scegliere l'accessorio FTD a cui applicare le modifiche e fare clic su **Deploy** per avviare la distribuzione dell'impostazione della piattaforma.

Syslog di limitazione della velocità

L'opzione Limite di velocità definisce il numero di messaggi che possono essere inviati a tutte le destinazioni configurate e definisce la severità del messaggio a cui si desidera assegnare i limiti di velocità.

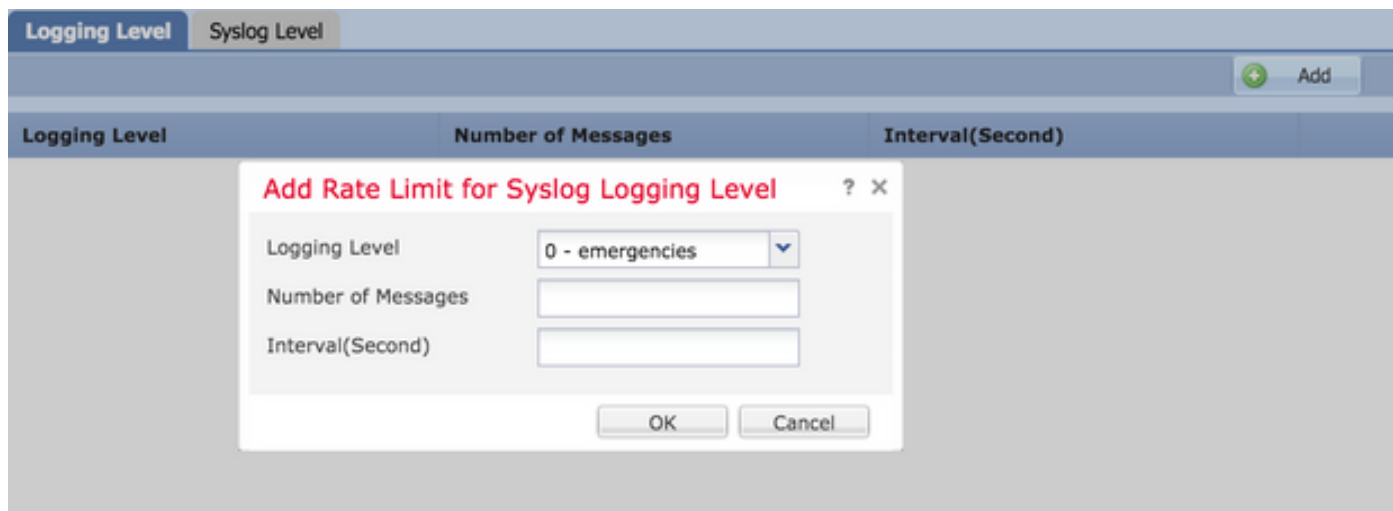
Per configurare elenchi di eventi personalizzati, scegliere **Device > Platform Setting > Threat Defense Policy > Syslog > Rate Limit**. Sono disponibili due opzioni in base alle quali è possibile specificare il limite di tasso:

- Livello di registrazione
- Livelli syslog

Per abilitare il limite di velocità basato sul livello di registrazione, scegliere **Logging Level** e fare clic su **Add**.

- **Logging Level:** dal **Logging Level** dall'elenco a discesa, scegliere il livello di log per il quale si desidera limitare la velocità.
- **Number of Messages:** immettere il numero massimo di messaggi Syslog da ricevere entro l'intervallo specificato.
- **Interval(Second):** in base al parametro Numero di messaggi configurato in precedenza, immettere l'intervallo di tempo durante il quale è possibile ricevere un insieme fisso di messaggi Syslog.

La velocità di Syslog è il numero di messaggi/intervalli.

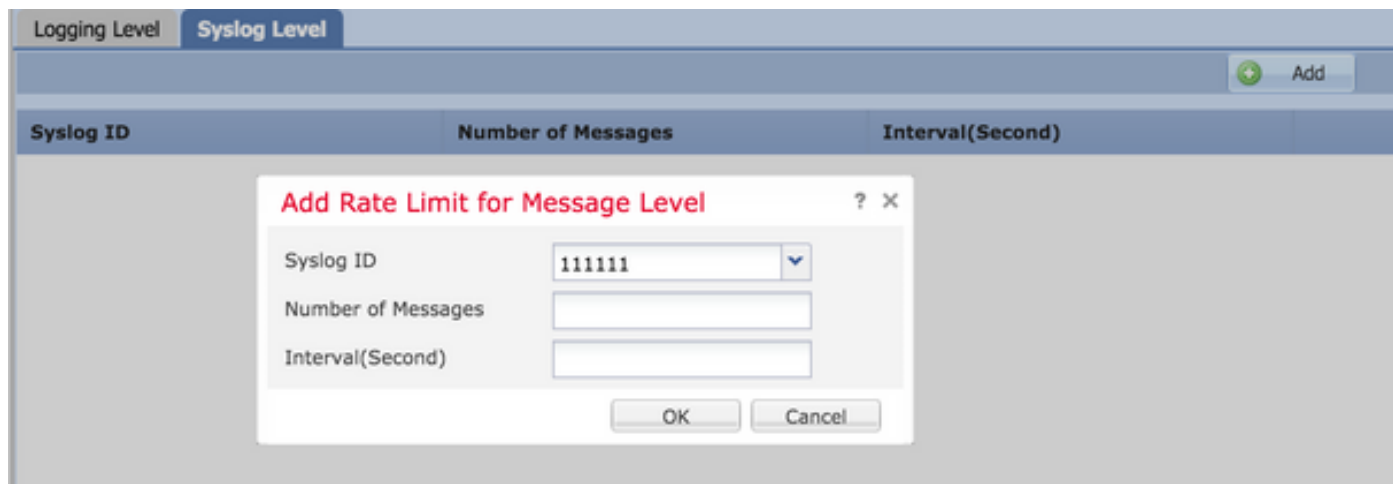


Fare clic su **OK** per salvare la configurazione del livello di log.

Per abilitare il limite di velocità basato sul livello di registrazione, scegliere **Logging Level** e fare clic su **Add**.

- **Syslog ID:** gli ID syslog vengono utilizzati per identificare in modo univoco i messaggi syslog. Dal **Syslog ID** dall'elenco a discesa, scegliere l'ID syslog.
- **Number of Messages:** immettere il numero massimo di messaggi syslog da ricevere entro l'intervallo specificato.
- **Interval(Second):** in base al parametro Numero di messaggi configurato in precedenza, immettere l'intervallo di tempo durante il quale è possibile ricevere un insieme fisso di messaggi Syslog.

La velocità di Syslog è il numero di messaggi/intervallo.



Fare clic su **OK** per salvare la configurazione a livello di syslog.

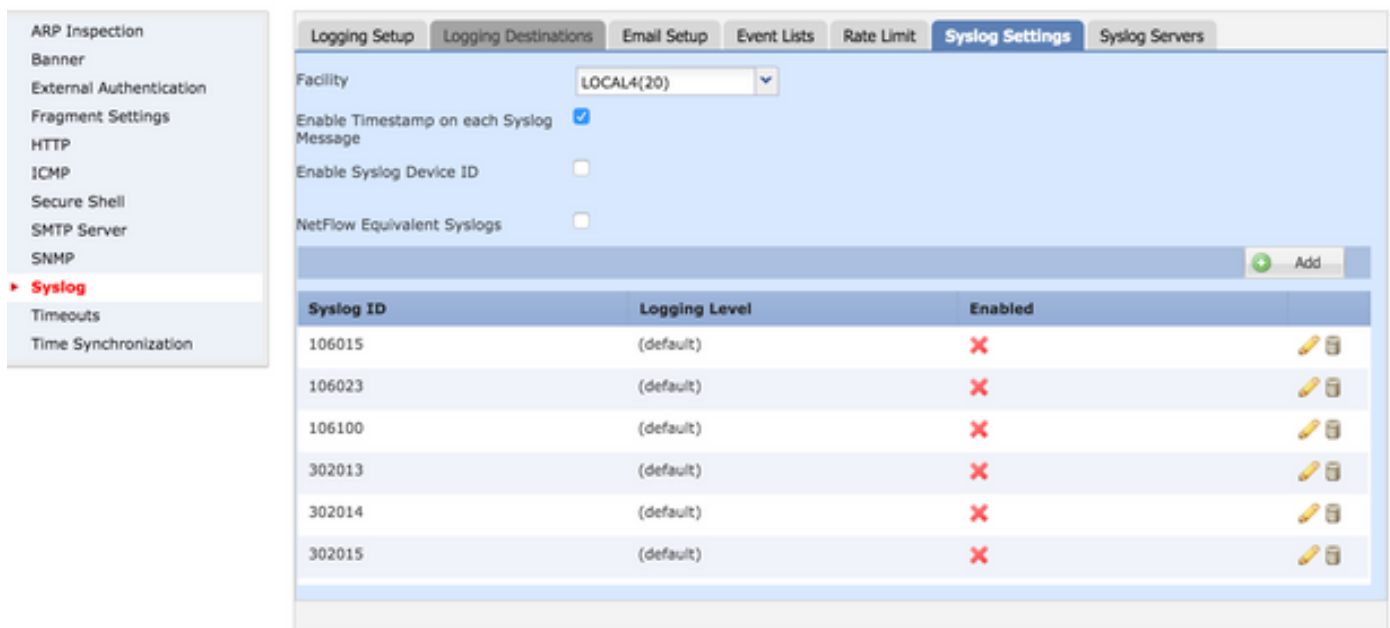
Fare clic su **Save** per salvare l'impostazione della piattaforma. Scegli di **Deploy**, scegliere l'accessorio FTD a cui applicare le modifiche e fare clic su **Deploy** per avviare la distribuzione dell'impostazione della piattaforma.

Impostazioni syslog

Le impostazioni Syslog consentono di configurare i valori della funzione da includere nei messaggi Syslog. È inoltre possibile includere l'indicatore orario nei messaggi di log e in altri parametri specifici del server Syslog.

Per configurare elenchi di eventi personalizzati, scegliere **Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Settings**.

- **Facility:** il codice della struttura consente di specificare il tipo di programma che registra il messaggio. I messaggi con funzionalità diverse possono essere gestiti in modo diverso. Dal **Facility** scegliere il valore della struttura.
- **Enable Timestamp on each Syslog Message:** controllare la **Enable Timestamp on each Syslog Message** per includere l'indicatore orario nei messaggi Syslog.
- **Enable Syslog Device ID:** controllare la **Enable Syslog Device ID** per includere un ID di periferica nei messaggi Syslog non in formato EMBLEM.
- **Netflow Equivalent Syslogs:** controllare la **Netflow Equivalent Syslogs** per inviare Syslog equivalenti a NetFlow. Può influire sulle prestazioni dell'accessorio.
- **Add Specific Syslog ID (Aggiungi ID syslog specifico):** per specificare l'ID syslog aggiuntivo, fare clic su **Add** e specificare il **Syslog ID/ Logging Level**.



The screenshot displays the 'Syslog Settings' configuration page. On the left is a navigation menu with 'Syslog' selected. The main content area has tabs for 'Logging Setup', 'Logging Destinations', 'Email Setup', 'Event Lists', 'Rate Limit', 'Syslog Settings' (active), and 'Syslog Servers'. The 'Facility' is set to 'LOCAL4(20)'. The 'Enable Timestamp on each Syslog Message' checkbox is checked. The 'Enable Syslog Device ID' and 'NetFlow Equivalent Syslogs' checkboxes are unchecked. Below these settings is a table with columns 'Syslog ID', 'Logging Level', and 'Enabled'. The table contains six rows, each with a Syslog ID, '(default)' as the logging level, and a red 'X' in the 'Enabled' column. To the right of the table is an 'Add' button.

Syslog ID	Logging Level	Enabled
106015	(default)	✗
106023	(default)	✗
106100	(default)	✗
302013	(default)	✗
302014	(default)	✗
302015	(default)	✗

Fare clic su **Save** per salvare l'impostazione della piattaforma. Scegli di **Deploy**, scegliere l'accessorio FTD a cui applicare le modifiche e fare clic su **Deploy** per avviare la distribuzione dell'impostazione della piattaforma.

Configura registrazione locale

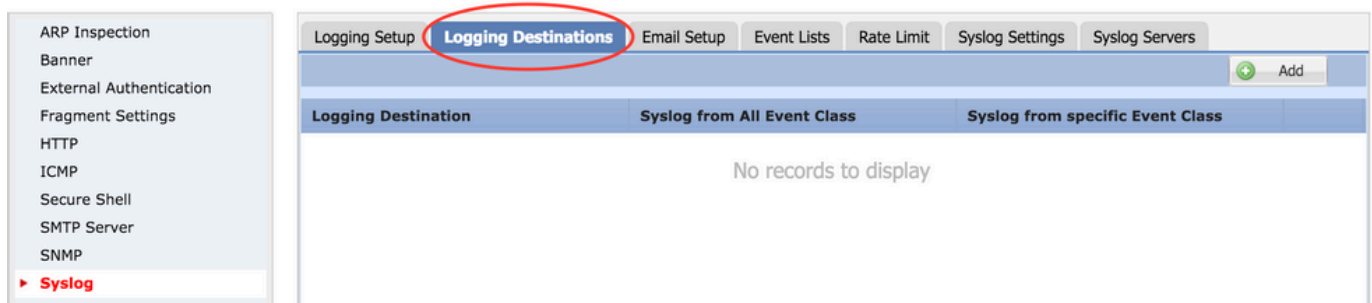
La sezione Destinazione di registrazione può essere utilizzata per configurare la registrazione su destinazioni specifiche.

Le destinazioni di registrazione interna disponibili sono:

- Buffer interno: esegue il log nel buffer di log interno (buffer di log)
- Console: invia i registri alla console (console di registrazione)
- Sessioni SSH: registra il syslog nelle sessioni SSH (terminal monitor)

Per configurare la registrazione locale, è necessario eseguire tre passaggi.

Passaggio 1. Scegli **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations**.



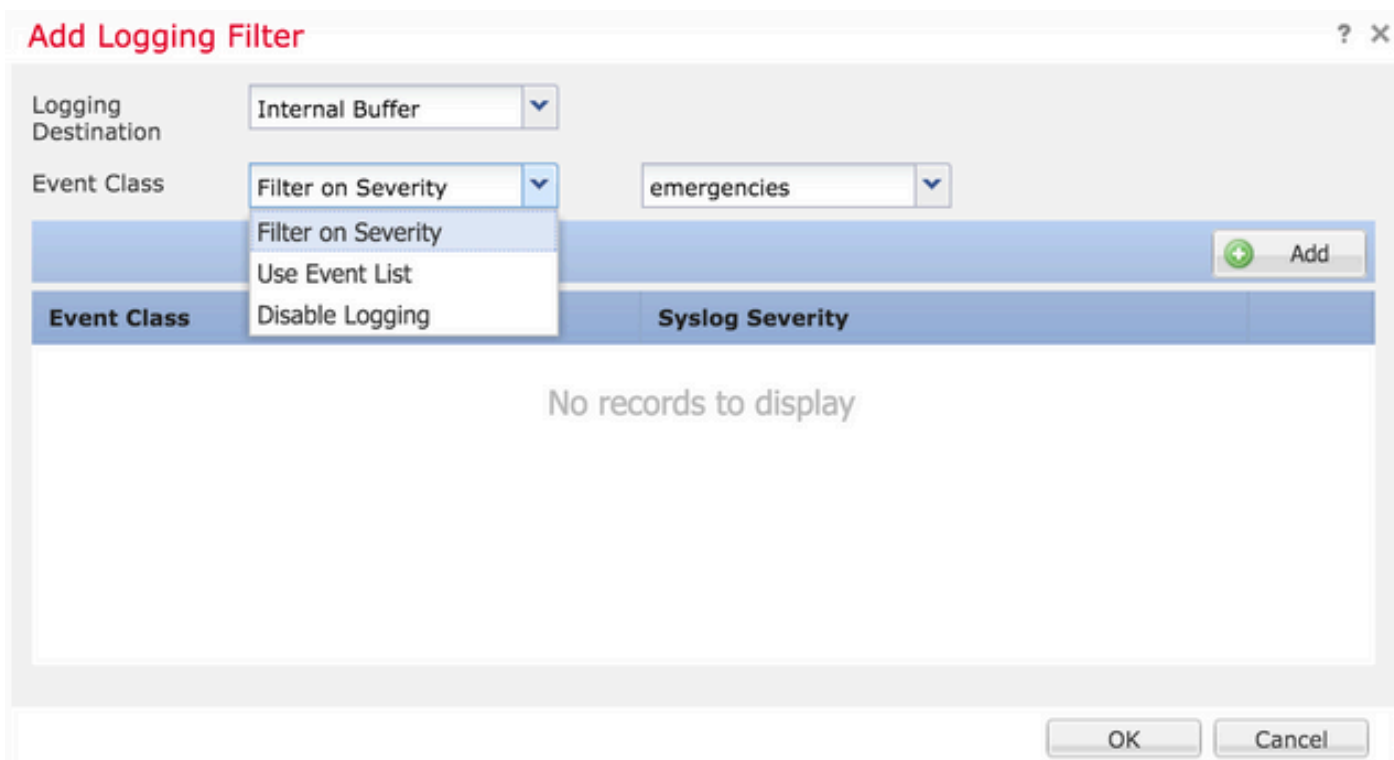
Passaggio 2. Fare clic su **Add** per aggiungere un filtro di registrazione per un **logging destination**.

Destinazione registrazione: scegliere la destinazione di registrazione richiesta dalla scheda **Logging Destination** come Buffer interno, Console o sessioni SSH.

Classe evento: da **Event Class** scegliere una classe Event. Come descritto in precedenza, le classi di evento sono un insieme di syslog che rappresentano le stesse funzionalità. Le classi di evento possono essere selezionate nei modi seguenti:

- Filter on Severity: le classi di evento filtrano in base alla gravità dei syslog.
- User Event List: gli amministratori possono creare elenchi di eventi specifici (descritti in precedenza) con classi di eventi personalizzate e farvi riferimento in questa sezione.
- Disable Logging: utilizzare questa opzione per disabilitare la registrazione per la destinazione e il livello di registrazione scelti.

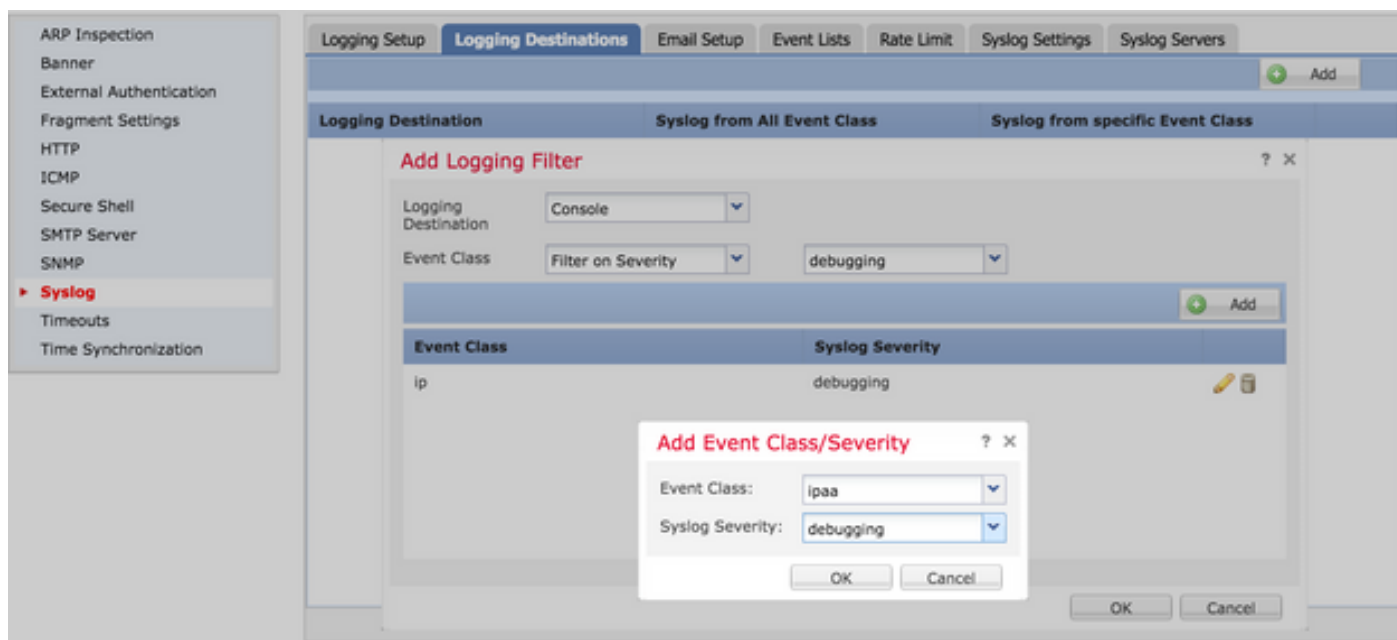
Livello di log: scegliere il livello di log dall'elenco a discesa. L'intervallo del livello di registrazione è compreso tra 0 (emergenze) e 7 (debug).



Passaggio 3. Per aggiungere una classe Event separata a questo filtro di registrazione, fare clic su **Add**.

Event Class: scegliere la classe di evento dal menu **Event Class** elenco a discesa.

Syslog Severity: scegliere il livello di gravità Syslog **Syslog Severity** elenco a discesa.



Fare clic su **OK** una volta configurato il filtro per aggiungere il filtro per una destinazione di registrazione specifica.

Fare clic su **Save** per salvare l'impostazione della piattaforma. Scegli **Deploy**, scegliere l'accessorio FTD a cui applicare le modifiche e fare clic su **Deploy** per avviare la distribuzione dell'impostazione

della piattaforma.

Configurare la registrazione esterna

Per configurare la registrazione esterna, scegliere **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations**.

FTD supporta questi tipi di registrazione esterna.

- Syslog Server: invia i log al server Syslog remoto.
- Trap SNMP: invia i log out come trap SNMP.
- E-mail: invia i log via e-mail con un server di inoltro della posta preconfigurato.

La configurazione per la registrazione esterna e la registrazione interna sono le stesse. La selezione delle destinazioni di logging determina il tipo di logging implementato. È possibile configurare le classi di evento basate su elenchi di eventi personalizzati per il server remoto.

Server Syslog Remoto

I server Syslog possono essere configurati per analizzare e archiviare i log in remoto dall'FTD.

Per configurare i server Syslog remoti, è necessario eseguire tre passaggi.

Passaggio 1. Scegli **Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Servers**.

Passaggio 2. Configurare il parametro correlato al server Syslog.

- Consenti il passaggio del traffico utente quando il server syslog TCP non è attivo: se un server syslog TCP è stato distribuito nella rete e non è raggiungibile, il traffico di rete attraverso l'appliance ASA viene rifiutato. Questa opzione è applicabile solo quando il protocollo di trasporto tra l'ASA e il server Syslog è TCP. Controllare la **Allow user traffic to pass when TCP syslog server is down** per consentire il passaggio del traffico attraverso l'interfaccia quando il server Syslog non è attivo.
- Dimensione coda messaggi: la dimensione della coda messaggi è il numero di messaggi che vengono inseriti nella coda FTD quando il server Syslog remoto è occupato e non accetta messaggi di log. Il valore predefinito è 512 messaggi e il valore minimo è 1 messaggio. Se in questa opzione si specifica 0, la dimensione della coda è considerata illimitata.

[Logging Setup](#)
[Logging Destinations](#)
[Email Setup](#)
[Event Lists](#)
[Rate Limit](#)
[Syslog Settings](#)
Syslog Servers

Allow user traffic to pass when TCP syslog server is down

Message Queue Size(messages)* (0 - 8192 messages). Use 0 to indicate unlimited Queue Size

Interface	IP Address	Protocol	Port	EMBLEM
No records to display				

Passaggio 3. Per aggiungere server Syslog remoti, fare clic su **Add**.

IP Address: dal **IP Address** dall'elenco a discesa, scegliere un oggetto di rete contenente i server Syslog elencati. Se non è stato creato un oggetto di rete, fare clic sul segno più (+) per creare un nuovo oggetto.

Protocol: fare clic su **TCP** o **UDP** pulsante di opzione per la comunicazione Syslog.

Port: immettere il numero di porta del server Syslog. Per impostazione predefinita, è 514.

Log Messages in Cisco EMBLEM format(UDP only): fare clic sul pulsante **Log Messages in Cisco EMBLEM format (UDP only)** per attivare questa opzione se è necessario registrare i messaggi nel formato Cisco EMBLEM. Questa opzione è applicabile solo ai syslog basati su UDP.

Available Zones: immettere le aree di sicurezza su cui è raggiungibile il server Syslog e spostarlo nella colonna **Aree selezionate/Interfacce selezionate**.

Add Syslog Server

IP Address*

Protocol TCP UDP

Port (514 or 1025-65535)

Log Messages in Cisco EMBLEM format(UDP only)

Available Zones

Selected Zones/Interfaces

outside

Fare clic su **OK** e **Save** per salvare la configurazione.

Fare clic su **Save** per salvare l'impostazione della piattaforma. Scegli **Deploy**, scegliere l'accessorio FTD a cui applicare le modifiche e fare clic su **Deploy** per avviare la distribuzione dell'impostazione della piattaforma.

Configurazione e-mail per registrazione

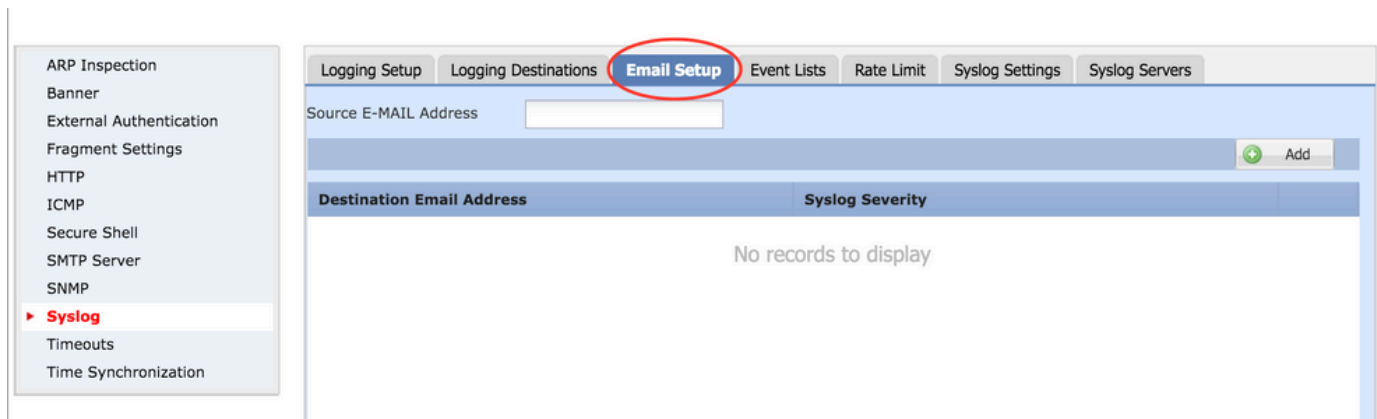
FTD consente di inviare il syslog a un indirizzo e-mail specifico. La posta elettronica può essere utilizzata come destinazione di registrazione solo se è già stato configurato un server di inoltro e-mail.

È possibile configurare le impostazioni di posta elettronica per i syslog in due passaggi.

Passaggio 1. Scegli **Device > Platform Setting > Threat Defense Policy > Syslog > Email Setup**.

Source E-MAIL Address: immettere l'indirizzo e-mail di origine che viene visualizzato su tutti i messaggi

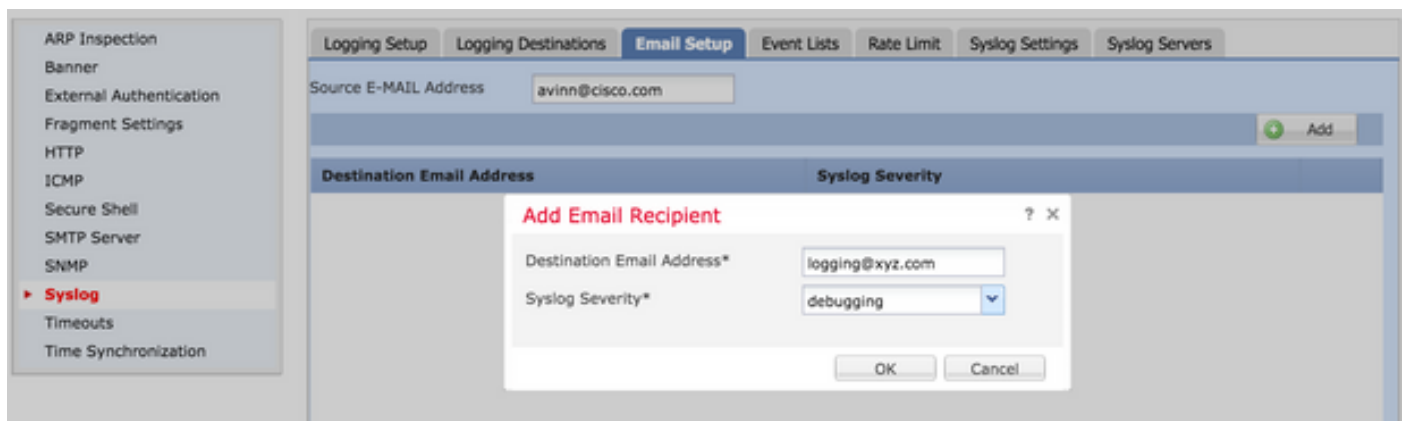
e-mail inviati dall'FTD che contengono i syslog.



Passaggio 2. Per configurare l'indirizzo e-mail di destinazione e la gravità del syslog, fare clic su **Add**.

Destination Email Address: immettere l'indirizzo e-mail di destinazione a cui inviare i messaggi Syslog.

Syslog Severity: scegliere il livello di gravità Syslog Syslog Severity elenco a discesa.



Fare clic su **OK** per salvare la configurazione.

Fare clic su **Save** per salvare l'impostazione della piattaforma. Scegli **Deploy**, scegliere l'accessorio FTD a cui applicare le modifiche e fare clic su **Deploy** per avviare la distribuzione dell'impostazione della piattaforma.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

- Verificare la configurazione del syslog FTD nella CLI FTD. Accedere all'interfaccia di

gestione dell'FTD e immettere il `system support diagnostic-cli` per accedere alla CLI di diagnostica.

```
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
><Press Enter>
firepower# sh run logging
logging enable
logging console emergencies
logging buffered debugging
logging host inside 192.168.0.192
logging flash-minimum-free 1024
logging flash-maximum-allocation 3076
logging permit-hostdown
```

- Accertarsi che il server Syslog sia raggiungibile dall'FTD. Accedere all'interfaccia di gestione FTD tramite SSH e verificare la connettività con `ping`

```
Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.
Cisco Fire Linux OS v6.0.1 (build 37)
Cisco Firepower Threat Defense for VMWare v6.0.1 (build 1213)
```

```
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower# ping 192.168.0.192
```

- È possibile acquisire un pacchetto per verificare la connettività tra l'FTD e il server Syslog. Accedere all'interfaccia di gestione FTD tramite SSH e immettere il comando `system support diagnostic-cli`. Per i comandi di acquisizione dei pacchetti, consultare l'[esempio di acquisizione dei pacchetti ASA con CLI e configurazione ASDM](#).
- Verificare che la distribuzione dei criteri sia stata applicata correttamente.

Informazioni correlate

- [Guida rapida di Cisco Firepower Threat Defense per l'appliance ASA](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

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).