

Konfigurieren von Geräten zum Senden und Anzeigen von Fehlerbehebungs-Syslogs auf FMC

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Funktionsüberblick](#)

[Konfigurieren](#)

[Überprüfen der Konfiguration](#)

Einleitung

In diesem Dokument wird beschrieben, wie verwaltete Geräte so konfiguriert werden, dass sie Syslog-Diagnosemeldungen an FMC senden und diese in der Unified Event Viewer anzeigen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Dieses Dokument gilt für alle Firepower-Plattformen.
- Secure Firewall Threat Defense Virtual (FTD) mit der Softwareversion 7.6.0
- Secure Firewall Management Center Virtual (FMC) mit der Softwareversion 7.6.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Funktionsüberblick

In Secure Firewall 7.6 wird der neue Fehlerbehebungsereignistyp in der Tabelle Unified Event Viewer hinzugefügt. Die Syslog-Protokollierungskonfiguration für die Plattformeinstellungen wurde erweitert. Sie unterstützt das Senden von LINA-generierten Syslog-Diagnosemeldungen an das FMC anstelle von VPN-Protokollen. Diese Funktion kann auf jedem FTD konfiguriert werden, auf dem eine mit FMC 7.6.0 kompatible Softwareversion ausgeführt wird. cdFMC wird nicht unterstützt, da cdFMC nicht über Analysetools verfügt.

- Die Option "Alle Protokolle" ist aufgrund des Ereignisvolumens auf Notruf-, Alarm- und kritische Protokollstufen beschränkt.
- Diese Fehlerbehebungsprotokolle zeigen alle Syslog-Protokolle an, die vom Gerät an das FMC (VPN oder andere) gesendet wurden.
- Die Fehlerbehebungsprotokolle werden an das FMC übertragen und sind in der einheitlichen Ereignisansicht und unter Geräte > Fehlerbehebung > Fehlerbehebungsprotokolle sichtbar.

Konfigurieren

Navigieren Sie zu FMC Devices > Platform Settings, und klicken Sie oben rechts in der Richtlinie auf das Symbol Edit (Bearbeiten).

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 present. The left sidebar contains navigation links for Home, Overview, Analysis, Policies, and Devices. The main content area displays a table titled "Platform Settings". The table has three columns: "Platform Settings", "Device Type", and "Status". A single row is visible with the following data: "FTD1_platform_settings" in the first column, "Threat Defense" in the second column, and "Targeting 1 device(s) Up-to-date on all targeted devices" in the third column. To the right of the status text, there are three icons: a document, a pencil (highlighted with a red box), and a trash can. A "New Policy" button is located in the top right corner of the main content area.

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

Richtlinie für Plattformeinstellungen

Wechseln Sie zu Syslog > Logging Setup. Unter Protokollierung beim sicheren Firewall-Management-Center werden drei Optionen angezeigt.

FTD1_platform_settings Save Cancel

Enter Description

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

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

2 - critical

FTP Server Information

☐ FTP server buffer wrap

Drei Protokollierungsoptionen

Wenn Sie Alle Protokolle auswählen, können Sie eine der drei verfügbaren Protokollierungsebenen auswählen: Notfälle, Warnungen und kritische Meldungen aus und senden alle Syslog-Diagnosemeldungen an FMC (einschließlich VPN).

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

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

2 - critical

0 - emergencies

1 - alerts

2 - critical

Available Interface Groups C

Selected Interface Groups

Verfügbare Protokollierungsebenen

Wenn Sie VPN-Protokolle auswählen, sind alle Protokollierungsebenen verfügbar, und eine davon kann ausgewählt werden.

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

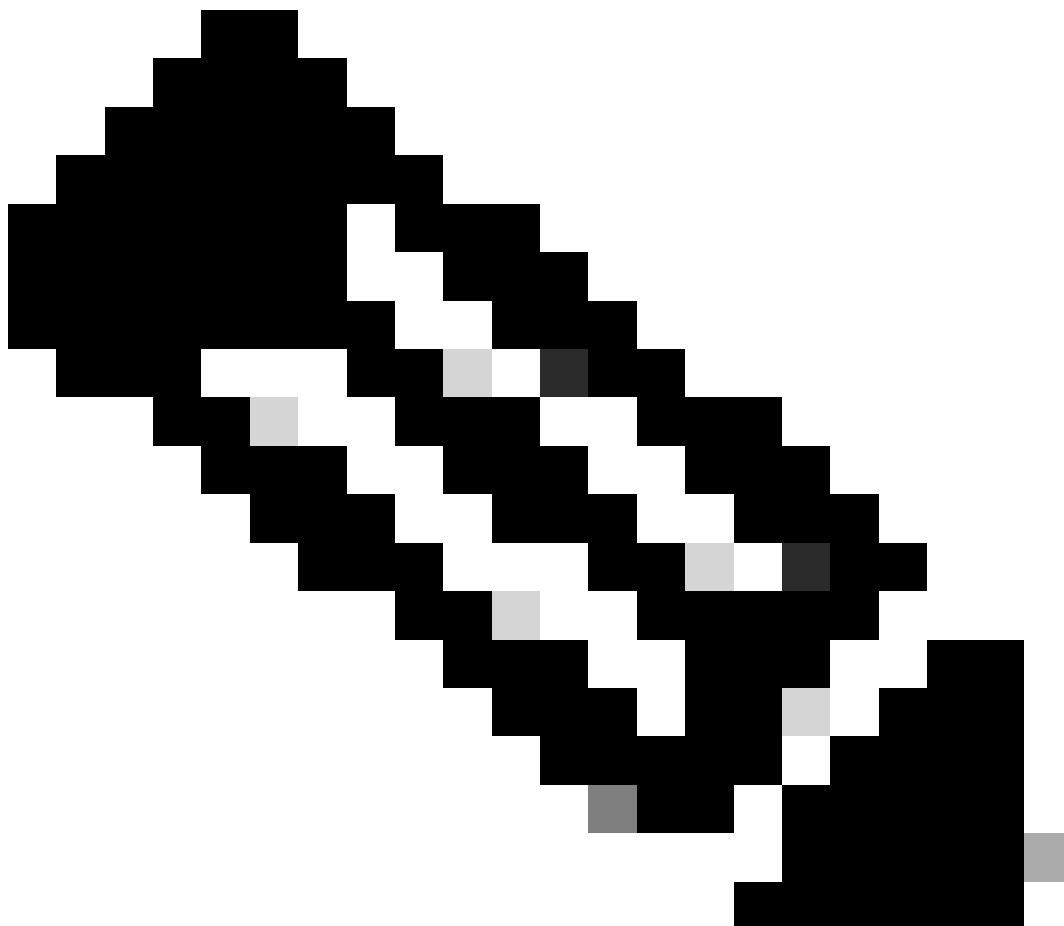
Available Interface Groups

Q Search

Add

Selected Interface Groups

Verfügbare Protokollierungsebenen



Anmerkung: Wenn Sie ein Gerät mit Site-to-Site- oder Remote Access-VPN konfigurieren,

aktiviert es standardmäßig automatisch das Senden von VPN-Syslogs an das Management Center. Sie können sie in All Logs (Alle Protokolle) ändern, um alle Syslogs außer den VPN-Protokollen an FMC zu senden.

Auf diese Protokolle kann von Devices (Geräte) > Troubleshoot (Fehlerbehebung) > Troubleshooting Logs (Fehlerbehebungsprotokolle) zugegriffen werden.

Firewall Management Center

Devices / Troubleshoot / Troubleshooting Logs

Q Search

Deploy



admin

Home

Overview

Analysis

Policies

Devices

Objects

Integration

Bookmark This Page | Create Report | Dashboard | View Bookmarks | Search

2025-01-15 15:33:00 - 2025-01-16 16:49:00

Static

No Search Constraints (Edit Search)

Table View of Troubleshooting Logs

☐	Time	Severity	Message	Message Class	Username	Device
☐	2025-01-15 19:59:43	Alert	(Primary) No response from other firewall (reason code = 4).	ha		FTD1
☐	2025-01-15 19:59:27	Alert	(Secondary) Disabling failover.	ha		FTD2
☐	2025-01-15 19:59:13	Alert	(Primary) No response from other firewall (reason code = 3).	ha		FTD1
☐	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
☐	2025-01-15 19:42:58	Alert	(Primary) No response from other firewall (reason code = 4).	ha		FTD1
☐	2025-01-15 19:42:54	Alert	(Secondary) No response from other firewall (reason code = 4).	ha		FTD2
☐	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

Tabellenansicht der Fehlerbehebungsprotokolle

Eine neue Registerkarte für die Fehlerbehebungsansicht ist jetzt auf der Seite Unified Event Viewer verfügbar. Um diese Ereignisse anzuzeigen, navigieren Sie zu Analyse > Vereinheitlichte Ereignisse > Problembehandlung.

Firewall Management Center
 Analysis / Unified Events

Deploy

admin ▾

Home

Overview

Analysis

Policies

Devices

Objects

Integration

Events

Troubleshooting

Refresh

14
0
0
0
0
14 events
2025-01-16 15:33:44 IST
2025-01-16 16:49:44 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

Fehlerbehebungsansicht

Sobald Sie zu dieser Registerkarte wechseln, wird ein neuer Ereignistyp in der Tabelle angezeigt. Sie kann nicht wie die anderen Typen zur Ansicht hinzugefügt oder daraus entfernt werden, da sie für die Fehlerbehebungsansicht von zentraler Bedeutung ist.

Firewall Management Center
 Analysis / Unified Events

Deploy

admin ▾

Home

Overview

Analysis

Policies

Devices

Objects

Integration

Events

Troubleshooting

Refresh

399
0
0
0
0
399 events
2025-01-15 15:33:44 IST
2025-01-16 16:49:44 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

Fehlerbehebung Ereignistyp

Andere Ereignistypen können weiterhin in dieser Fehlerbehebungsansicht hinzugefügt und entfernt werden. Dadurch können Sie Diagnoseprotokolle zusammen mit anderen Ereignisdaten anzeigen.

Firewall Management Center

Analysis / Unified Events

Search

Deploy

admin

Home

Overview

Analysis

Policies

Devices

Objects

Integration

Events

Troubleshooting

Event Type

Troubleshooting

Connection

Intrusion

Refresh

399

14

0

413 events

2025-01-15 15:33:44 IST

2025-01-16 16:49:44 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

Andere Ereignistypen

Überprüfen der Konfiguration

Nachdem die Konfiguration über die FMC-GUI vorgenommen wurde, kann sie über die FTD-CLI überprüft werden, indem die Befehle `show running-config logging` und `show logging` entweder im CLISH- oder im LINA-Modus ausgeführt werden.

```
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-Befehl

```
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-Befehl

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.