

# Konfigurieren der Protokollierung auf FTD über FMC

## Inhalt

- [Einleitung](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Hintergrundinformationen](#)
- [Konfigurieren](#)
- [Globale Syslog-Konfiguration konfigurieren](#)
- [Protokoll-Setup](#)
- [Ereignislisten](#)
- [Syslog zur Ratenbegrenzung](#)
- [Syslog-Einstellungen](#)
- [Lokale Protokollierung konfigurieren](#)
- [Konfigurieren der externen Protokollierung](#)
- [Remote-Syslog-Server](#)
- [E-Mail-Einrichtung für Protokollierung](#)
- [Überprüfung](#)
- [Fehlerbehebung](#)
- [Zugehörige Informationen](#)

## Einleitung

Dieses Dokument behandelt die Protokollierungskonfiguration im Firepower Management Center (FMC) für Firepower Threat Defense (FTD).

## Voraussetzungen

### Anforderungen

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

- FirePOWER-Technologie
- Adaptive Security Appliance (ASA)
- Syslog Protokoll

### Verwendete Komponenten

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

- ASA Firepower Threat Defense-Image für ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X ) mit Softwareversion 6.0.1 und höher
- ASA Firepower Threat Defense-Image für ASA (5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) mit Softwareversion 6.0.1 und höher
- FMC Version 6.0.1 und höher

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.

## Hintergrundinformationen

Die FTD-Systemprotokolle liefern Ihnen die Informationen, die Sie zur Überwachung und Fehlerbehebung der FTD-Einheit benötigen.

Die Protokolle sind sowohl für die routinemäßige Fehlerbehebung als auch für die Behandlung von Vorfällen nützlich. Die FTD-Appliance unterstützt sowohl lokale als auch externe Protokollierung.

Die lokale Protokollierung kann Ihnen bei der Behebung von Live-Problemen helfen. Die externe Protokollierung ist eine Methode zum Sammeln von Protokollen von der FTD-Appliance an einen externen Syslog-Server.

Durch die Protokollierung auf einem zentralen Server können Protokolle und Warnungen aggregiert werden. Externe Protokollierung kann bei der Protokollkorrelation und der Behandlung von Vorfällen helfen.

Für die lokale Protokollierung unterstützt die FTD-Appliance die Konsole, die Option für den internen Puffer und die SSH-Sitzungsprotokollierung (Secure Shell).

Für die externe Protokollierung unterstützt die FTD-Appliance den externen Syslog-Server und den E-Mail-Relay-Server.

---

**Hinweis:** Wenn ein hohes Datenverkehrsvolumen die Appliance passiert, achten Sie auf die Art der Protokollierung/den Schweregrad/Ratenbegrenzung. Führen Sie diese Schritte aus, um die Anzahl der Protokolle zu begrenzen, sodass die Firewall nicht beeinträchtigt wird.

---

## Konfigurieren

Alle protokollbezogenen Konfigurationen können konfiguriert werden, wenn Sie zum [Platform Settings](#) Unterfenster [Devices](#) aus. Auswählen [Devices](#) > [Platform Settings](#) wie in diesem Bild dargestellt.



Klicken Sie auf das Bleistiftsymbol, um die vorhandene Richtlinie zu bearbeiten, oder klicken Sie auf [New Policy](#), und wählen Sie [Threat Defense Settings](#) um eine neue FTD-Richtlinie zu erstellen, wie in diesem Bild gezeigt.

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

Wählen Sie die FTD-Appliance aus, um diese Richtlinie anzuwenden, und klicken Sie auf **Save** wie in diesem Bild dargestellt.

## Globale Syslog-Konfiguration konfigurieren

Es gibt bestimmte Konfigurationen, die für die lokale und die externe Protokollierung anwendbar sind. Dieser Abschnitt behandelt die obligatorischen und optionalen Parameter, die für Syslog konfiguriert werden können.

### Protokoll-Setup

Die Protokollierungseinrichtungsoptionen gelten für die lokale und externe Protokollierung. Um das Protokoll-Setup zu konfigurieren, wählen Sie **Devices > Platform Settings**.

Auswählen **Syslog > Logging Setup**.

### Grundlegende Einrichtung der Protokollierung

- **Enable Logging:** Überprüfen Sie die **Enable Logging** Kontrollkästchen, um die Protokollierung zu aktivieren. Dies ist eine obligatorische Option.
- **Enable Logging on the failover standby unit:** Überprüfen Sie die **Enable Logging on the failover standby unit** das

Kontrollkästchen, um die Protokollierung auf dem Standby-FTD zu konfigurieren, das Teil eines FTD-Hochverfügbarkeits-Clusters ist.

- **Send syslogs in EMBLEM format:** Überprüfen Sie die **Send syslogs in EMBLEM format** das Kontrollkästchen, um das Format von Syslog als EMBLEM für jedes Ziel zu aktivieren. Das EMBLEM-Format wird hauptsächlich für den Syslog-Analyzer CiscoWorks Resource Manager Essentials (RME) verwendet. Dieses Format entspricht dem Cisco IOS Software Syslog-Format, das von den Routern und Switches erstellt wurde. Sie ist nur für UDP-Syslog-Server verfügbar.
- **Send debug messages as syslogs:** Überprüfen Sie die **Send debug messages as syslogs** das Kontrollkästchen, um die Debug-Protokolle als Syslog-Meldungen an den Syslog-Server zu senden.
- **Memory size of the Internal Buffer:** Geben Sie die Größe des internen Speicherpuffers ein, in dem FTD die Protokolldaten speichern kann. Die Protokolldaten werden rotiert, wenn die Puffergrenze erreicht ist.

### **FTP-Serverinformationen (optional)**

Geben Sie FTP-Serverdetails an, wenn Sie die Protokolldaten an den FTP-Server senden möchten, bevor der interne Puffer überschrieben wird.

- **FTP Server Buffer Wrap:** Überprüfen Sie die **FTP Server Buffer Wrap** das Kontrollkästchen, um die Pufferprotokolldaten an den FTP-Server zu senden.
- **IP Address:** Geben Sie die IP-Adresse des FTP-Servers ein.
- **Username:** Geben Sie den Benutzernamen des FTP-Servers ein.
- **Path:** Geben Sie den Verzeichnispfad des FTP-Servers ein.
- **Password:** Geben Sie das Kennwort des FTP-Servers ein.
- **Confirm:** Geben Sie das gleiche Kennwort erneut ein.

### **Flash-Größe (optional)**

Geben Sie die Flash-Größe an, wenn Sie die Protokolldaten speichern möchten, sobald der interne Puffer voll ist.

- **Flash:** Überprüfen Sie die **Flash** , um die Protokolldaten an den internen Flash zu senden.
- **Maximum Flash to be used by Logging(KB):** Geben Sie die maximale Größe des Flash-Speichers in KB ein, der für die Protokollierung verwendet werden kann.
- **Minimum free Space to be preserved(KB):** Geben Sie die Mindestgröße des Flash-Speichers in KB ein, die beibehalten werden soll.

- ARP Inspection
- Banner
- External Authentication
- Fragment Settings
- HTTP
- ICMP
- Secure Shell
- SMTP Server
- SNMP
- **Syslog**
- Timeouts
- Time Synchronization

Logging Setup
Logging Destinations
Email Setup
Event Lists
Rate Limit
Syslog

**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  (4096-52428800 Bytes)

**Specify FTP Server Information**

FTP Server Buffer Wrap

IP Address\*  ▼

Username\*

Path\*

Password\*

Confirm\*

**Specify Flash Size**

Flash

Maximum Flash to be used by Logging(KB)  (4-8044176)

Minimum free Space to be preserved(KB)  (0-8044176)

Klicken Sie auf **save** um die Plattformeinstellung zu speichern. Wählen Sie **Deploy** wählen Sie die FTD-Appliance aus, auf die Sie die Änderungen anwenden möchten, und klicken Sie auf **Deploy** um mit der Bereitstellung der Plattformeinstellung zu beginnen.

## Ereignislisten

Mit der Option Ereignislisten konfigurieren können Sie eine Ereignisliste erstellen/bearbeiten und angeben, welche Protokolldaten in den Ereignislistenfilter aufgenommen werden sollen. Ereignislisten können verwendet werden, wenn Sie unter Protokollierungsziele Protokollierungsfilter konfigurieren.

Das System bietet zwei Optionen zur Verwendung der Funktionen benutzerdefinierter Ereignislisten.

- Klasse und Schweregrad
- Nachrichten-ID

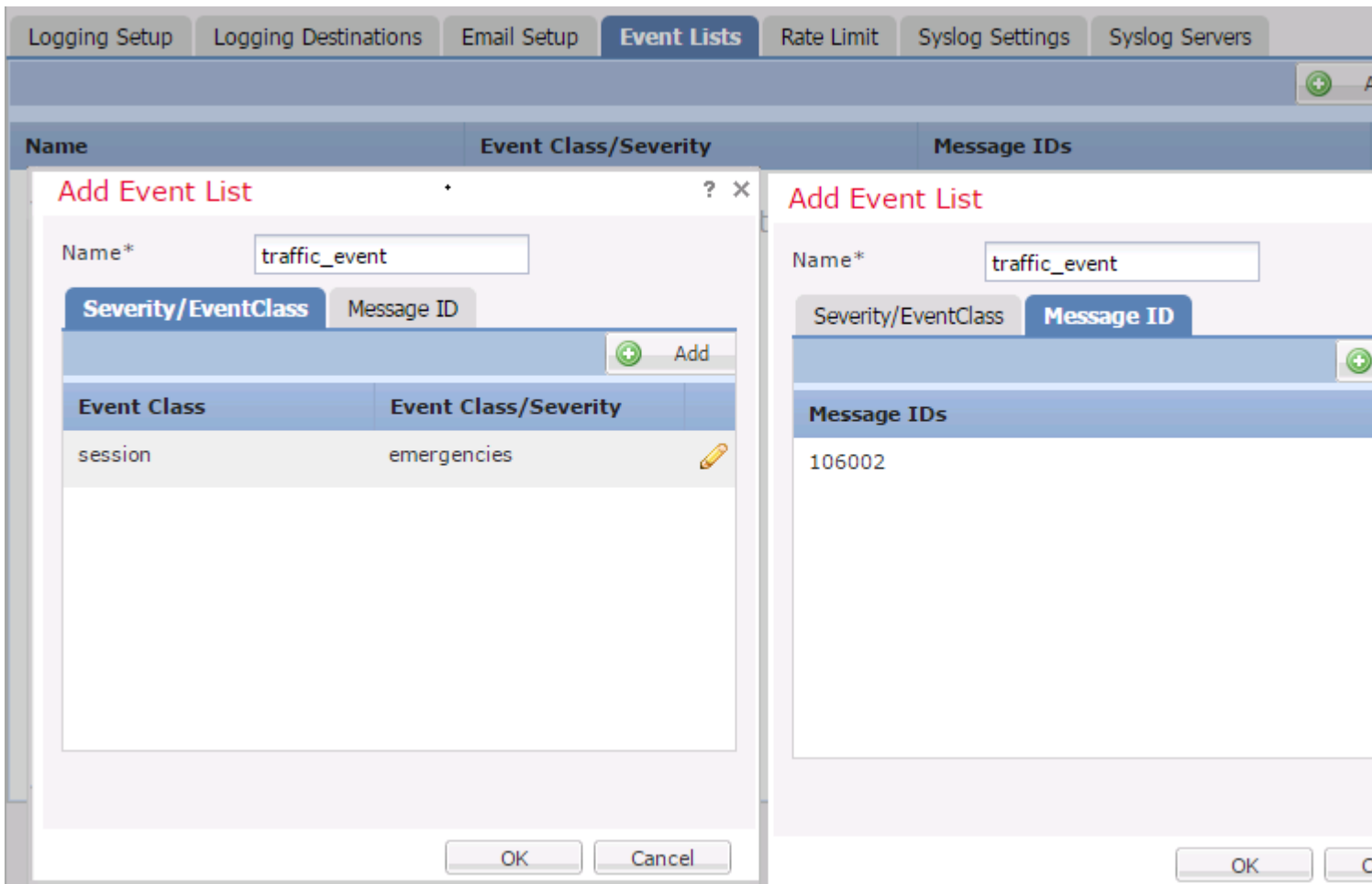
Um benutzerdefinierte Ereignislisten zu konfigurieren, wählen Sie **Device > Platform Setting > Threat Defense Policy > Syslog > Event List** und klicke auf **Add**. Folgende Optionen stehen zur Verfügung:

- Name: Geben Sie den Namen der Ereignisliste ein.
- Severity/Event Class: Klicken Sie im Abschnitt Severity/Event Class (Schweregrad/Ereignisklasse) auf **Add**.
- Event Class: Wählen Sie aus der Dropdown-Liste die Ereignisklasse für den gewünschten

Protokolldatentyp aus. Eine Event Class definiert einen Satz von Syslog-Regeln, die dieselben Funktionen darstellen.

Es gibt z. B. eine Event Class für die Sitzung, die alle Syslogs enthält, die sich auf die Sitzung beziehen.

- Syslog Severity: Wählen Sie den Schweregrad aus der Dropdown-Liste für die ausgewählte Ereignisklasse aus. Der Schweregrad kann zwischen 0 (Notfall) und 7 (Debugging) liegen.
- Message ID: Wenn Sie an bestimmten Protokolldaten zu einer Nachrichten-ID interessiert sind, klicken Sie auf **Add** um einen Filter basierend auf der Nachrichten-ID zu setzen.
- Message IDs: Geben Sie die Nachrichten-ID als Einzel-/Bereichsformat an.



Klicken Sie auf **OK** um die Konfiguration zu speichern.

Klicken Sie auf **Save** um die Plattformeinstellung zu speichern. Auswahl **Deploy**, wählen Sie die FTD-Einheit aus, auf die Sie die Änderungen anwenden möchten, und klicken Sie auf **Deploy** mit der Bereitstellung der Plattformeinstellung zu beginnen.

### Syslog zur Ratenbegrenzung

Die Option "Rate limit" legt die Anzahl der Nachrichten fest, die an alle konfigurierten Ziele gesendet werden können, sowie den Schweregrad der Nachricht, der Sie eine Rate Limits zuweisen möchten.

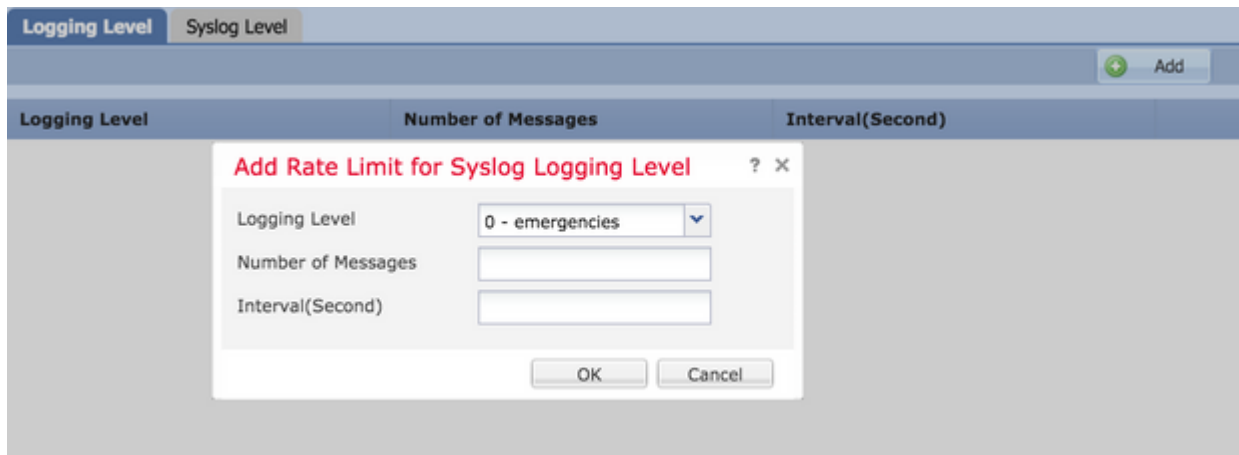
Um benutzerdefinierte Ereignislisten zu konfigurieren, wählen Sie **Device > Platform Setting > Threat Defense Policy > Syslog > Rate Limit**. Sie haben zwei Optionen, anhand derer Sie das Ratenlimit festlegen können:

- Protokollierende Stufe
- Syslog-Ebenen

Um das Durchsatzlimit für die Protokollierungsebene zu aktivieren, wählen Sie **Logging Level** und klicke auf **Add**.

- **Logging Level:** Aus dem **Logging Level** die Protokollierungsebene aus, für die die Ratenbegrenzung durchgeführt werden soll.
- **Number of Messages:** Geben Sie die maximale Anzahl von Syslog-Meldungen ein, die innerhalb des angegebenen Intervalls empfangen werden sollen.
- **Interval(Second):** Geben Sie basierend auf dem zuvor konfigurierten Parameter **Number of Messages** (Anzahl der Nachrichten) das Zeitintervall ein, in dem ein fester Satz von Syslog-Nachrichten empfangen werden kann.

Die Syslog-Rate entspricht der Anzahl der Nachrichten/Intervalle.



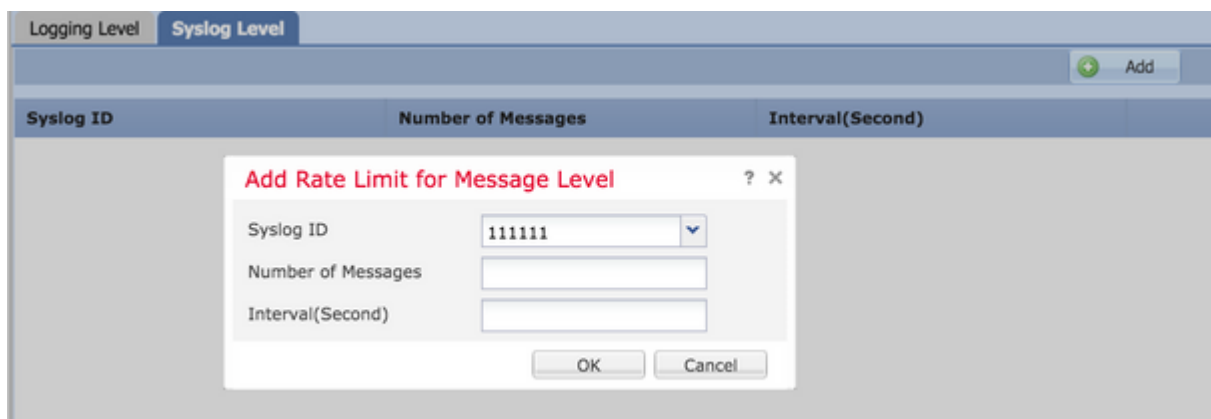
The screenshot shows a software interface with two tabs: "Logging Level" and "Syslog Level". The "Syslog Level" tab is active. Below the tabs is a table with three columns: "Logging Level", "Number of Messages", and "Interval(Second)". A modal dialog box titled "Add Rate Limit for Syslog Logging Level" is open in the foreground. It contains three input fields: "Logging Level" with a dropdown menu showing "0 - emergencies", "Number of Messages" with an empty text box, and "Interval(Second)" with an empty text box. At the bottom of the dialog are "OK" and "Cancel" buttons.

Klicken Sie auf **OK** um die Konfiguration der Protokollierungsebene zu speichern.

Um das Durchsatzlimit für die Protokollierungsebene zu aktivieren, wählen Sie **Logging Level** und klicke auf **Add**.

- **Syslog ID:** Syslog-IDs werden zur eindeutigen Identifizierung der Syslog-Meldungen verwendet. Über die **Syslog ID** die Syslog-ID aus.
- **Number of Messages:** Geben Sie die maximale Anzahl von Syslog-Meldungen ein, die innerhalb des angegebenen Intervalls empfangen werden sollen.
- **Interval(Second):** Geben Sie basierend auf dem zuvor konfigurierten Parameter **Number of Messages** (Anzahl der Nachrichten) das Zeitintervall ein, in dem ein fester Satz von Syslog-Nachrichten empfangen werden kann.

Die Syslog-Rate entspricht der Anzahl der Nachrichten/dem Intervall.



The screenshot shows a software interface with two tabs: "Logging Level" and "Syslog Level". The "Syslog Level" tab is active. Below the tabs is a table with three columns: "Syslog ID", "Number of Messages", and "Interval(Second)". A modal dialog box titled "Add Rate Limit for Message Level" is open in the foreground. It contains three input fields: "Syslog ID" with a dropdown menu showing "111111", "Number of Messages" with an empty text box, and "Interval(Second)" with an empty text box. At the bottom of the dialog are "OK" and "Cancel" buttons.

Klicken Sie auf **OK** um die Konfiguration auf Syslog-Ebene zu speichern.

Klicken Sie auf **save** um die Plattformeinstellung zu speichern. Auswahl **Deploy**, wählen Sie die FTD-Einheit aus, auf die Sie die Änderungen anwenden möchten, und klicken Sie auf **Deploy** um mit der Bereitstellung der Plattformeinstellung zu beginnen.

## Syslog-Einstellungen

Die Syslog-Einstellungen ermöglichen die Konfiguration der Anlagenwerte, die in die Syslog-Meldungen aufgenommen werden sollen. Sie können den Zeitstempel auch in Protokollmeldungen und andere serverspezifische Syslog-Parameter einfügen.

Um benutzerdefinierte Ereignislisten zu konfigurieren, wählen Sie **Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Settings**.

- Facility: Ein Einrichtungscode wird verwendet, um den Programmtyp anzugeben, der die Nachricht protokolliert. Nachrichten mit unterschiedlichen Einrichtungen können unterschiedlich behandelt werden. Über die **Facility** den Wert für die Einrichtung auswählen.
- Enable Timestamp on each Syslog Message: Überprüfen Sie die **Enable Timestamp on each Syslog Message** aktivieren, um den Zeitstempel in Syslog-Meldungen einzuschließen.
- Enable Syslog Device ID: Überprüfen Sie die **Enable Syslog Device ID** aktivieren, um eine Geräte-ID in Syslog-Meldungen einzuschließen, die nicht im EMBLEM-Format sind.
- Netflow Equivalent Syslogs: Überprüfen Sie die **Netflow Equivalent Syslogs** Kontrollkästchen, um NetFlow-äquivalente Syslogs zu senden. Sie kann die Leistung der Appliance beeinträchtigen.
- Spezifische Syslog-ID hinzufügen: Um die zusätzliche Syslog-ID anzugeben, klicken Sie auf **Add** und die **Syslog ID/ Logging Level** Kontrollkästchen.

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

Klicken Sie auf **save** um die Plattformeinstellung zu speichern. Auswahl **Deploy**, wählen Sie die FTD-Einheit aus, auf die Sie die Änderungen anwenden möchten, und klicken Sie auf **Deploy** um mit der Bereitstellung der Plattformeinstellung zu beginnen.

## Lokale Protokollierung konfigurieren

Der Abschnitt "Logging Destination" (Protokollierungsziel) kann verwendet werden, um die Protokollierung für bestimmte Ziele zu konfigurieren.

Folgende interne Protokollierungsziele sind verfügbar:

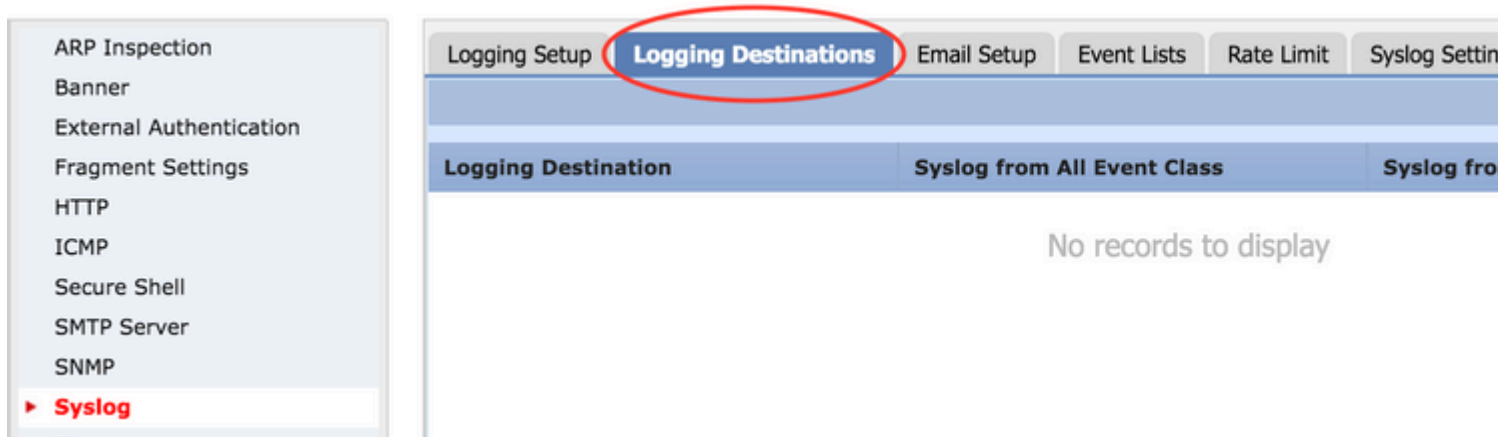
- Interner Puffer: Protokolliert im internen Protokollierungspuffer (gepufferte Protokollierung)



- Konsole: Sendet Protokolle an die Konsole (Protokollkonsole)
- SSH-Sitzungen: Protokollierung von Syslog in SSH-Sitzungen (Terminalmonitor)

Es gibt drei Schritte zum Konfigurieren der lokalen Protokollierung.

Schritt 1: Auswählen **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations**.



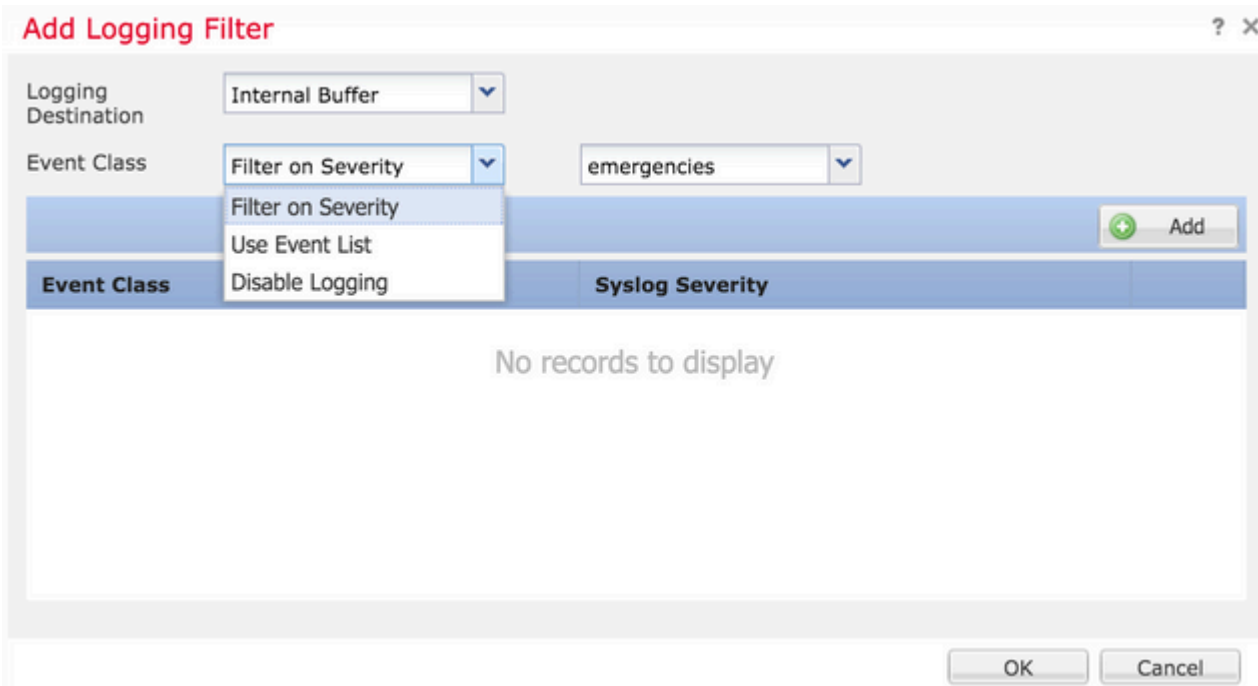
Schritt 2: Klicken Sie auf **Add** um einen Protokollierungsfilter für einen bestimmten **logging destination**.

Protokollierungsziel: Wählen Sie das erforderliche Protokollierungsziel aus dem **Logging Destination** als "Internal Buffer", "Console" oder SSH-Sitzungen.

Ereignisklasse: Aus dem **Event Class** eine Event-Klasse auswählen. Wie bereits beschrieben, handelt es sich bei Ereignisklassen um eine Reihe von Syslogs, die dieselben Funktionen darstellen. Ereignisklassen können folgendermaßen ausgewählt werden:

- Filter on Severity: Ereignisklassen filtern nach dem Schweregrad der Syslogs.
- User Event List: Administratoren können spezifische (zuvor beschriebene) Ereignislisten mit eigenen benutzerdefinierten Ereignisklassen erstellen und in diesem Abschnitt auf diese verweisen.
- Disable Logging: Verwenden Sie diese Option, um die Protokollierung für das ausgewählte Protokollierungsziel und die ausgewählte Protokollierungsebene zu deaktivieren.

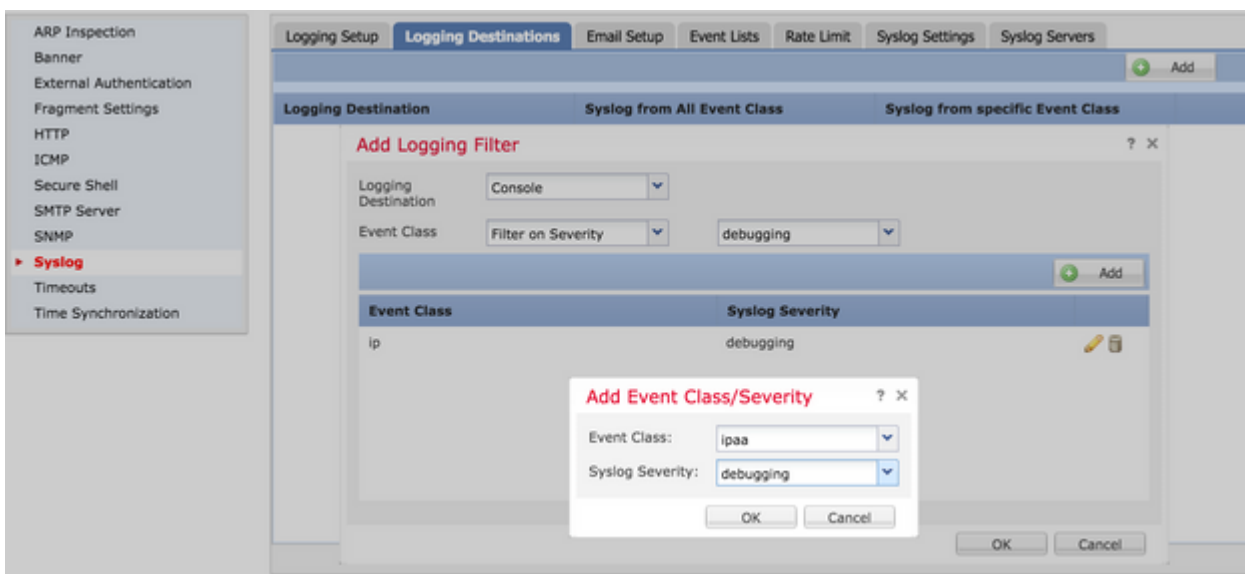
Protokollierungsebene: Wählen Sie die Protokollierungsebene aus der Dropdown-Liste aus. Der Bereich der Protokollierungsebene reicht von 0 (Notfälle) bis 7 (Debugging).



Schritt 3: Um diesem Protokollierungsfilter eine separate Ereignisklasse hinzuzufügen, klicken Sie auf **Add**.

Event Class: Wählen Sie die Ereignisklasse aus dem **Event Class** aus.

Syslog Severity: Wählen Sie den Syslog-Schweregrad aus dem **Syslog Severity** aus.



Klicken Sie auf **OK** sobald der Filter so konfiguriert wurde, dass er den Filter für ein bestimmtes Protokollierungsziel hinzufügt.

Klicken Sie auf **save** um die Plattformeinstellung zu speichern. Auswählen **Deploy**, wählen Sie die FTD-Einheit aus, auf die Sie die Änderungen anwenden möchten, und klicken Sie auf **Deploy** um die Bereitstellung der Plattformeinstellung zu starten.

## Konfigurieren der externen Protokollierung

Um die externe Protokollierung zu konfigurieren, wählen Sie **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations**.

FTD unterstützt diese externe Protokollierung.

- Syslog Server (Syslog-Server): Sendet Protokolle an den Remote-Syslog-Server.
- SNMP-Trap: Sendet die Abmeldungen als SNMP-Trap.
- E-Mail: Versendet die Protokolle per E-Mail mit einem vorkonfigurierten Mail-Relay-Server.

Die Konfiguration für die externe und die interne Protokollierung ist identisch. Die Auswahl der Protokollierungsziele bestimmt, welche Protokollierungsart implementiert wird. Es ist möglich, Ereignisklassen auf der Grundlage benutzerdefinierter Ereignislisten für den Remote-Server zu konfigurieren.

## Remote-Syslog-Server

Syslog-Server können so konfiguriert werden, dass sie Protokolle remote vom FTD analysieren und speichern.

Es gibt drei Schritte, um Syslog-Remote-Server zu konfigurieren.

Schritt 1: Auswählen **Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Servers**.

Schritt 2: Konfigurieren Sie den Syslog-Serverparameter.

- Benutzerdatenverkehr passieren lassen, wenn der TCP-Syslog-Server ausgefallen ist: Wenn ein TCP-Syslog-Server im Netzwerk bereitgestellt wurde und nicht erreichbar ist, wird der Netzwerkdatenverkehr über die ASA abgelehnt. Dies gilt nur, wenn das Transportprotokoll zwischen ASA und Syslog-Server TCP ist. Überprüfen Sie **Allow user traffic to pass when TCP syslog server is down** das Kontrollkästchen, damit der Datenverkehr die Schnittstelle passiert, wenn der Syslog-Server ausgefallen ist.
- Message Queue Size (Größe der Nachrichtenwarteschlange): Die Größe der Nachrichtenwarteschlange entspricht der Anzahl der Nachrichten, die in der FTD in die Warteschlange gestellt werden, wenn der entfernte Syslog-Server ausgelastet ist und keine Protokollnachrichten annimmt. Der Standardwert beträgt 512 Nachrichten und das Minimum ist 1 Nachricht. Wenn Sie für diese Option 0 angeben, wird die Warteschlangengröße als unbegrenzt betrachtet.

Interface	IP Address	Protocol	Port	EMBLEM
No records to display				

Schritt 3: Um Syslog-Remote-Server hinzuzufügen, klicken Sie **Add**.

IP Address: Aus dem **IP Address** ein Netzwerkobjekt auswählen, in dem die Syslog-Server aufgelistet sind. Wenn Sie kein Netzwerkobjekt erstellt haben, klicken Sie auf das Pluszeichen (+), um ein neues Objekt zu erstellen.

Protocol: Klicken Sie entweder auf **TCP** Oder **UDP** Optionsfeld für die Syslog-Kommunikation.

Port: Geben Sie die Portnummer des Syslog-Servers ein. Standardmäßig ist dies 514.

Log Messages in Cisco EMBLEM format(UDP only): Klicken Sie auf **Log Messages in Cisco EMBLEM format (UDP only)** aktivieren, um diese Option zu aktivieren, wenn Meldungen im Cisco EMBLEM-Format protokolliert werden müssen. Dies gilt nur für das UDP-basierte Syslog.

Available Zones: Geben Sie die Sicherheitszonen ein, über die der Syslog-Server erreichbar ist, und verschieben Sie ihn in die Spalte Ausgewählte Zonen/Schnittstellen.

The screenshot shows the 'Add Syslog Server' configuration window. The 'IP Address\*' field is set to 'SYSLOG\_SERVERS'. The 'Protocol' is set to 'UDP'. The 'Port' is set to '514'. The 'Log Messages in Cisco EMBLEM format(UDP only)' checkbox is unchecked. The 'Available Zones' pane is empty, and the 'Selected Zones/Interfaces' pane contains 'outside'. The 'Add' button is visible between the panes. The 'Interface Name' field is empty, and the 'Add' button is next to it. The 'OK' and 'Cancel' buttons are at the bottom.

Klicken Sie auf **OK** und **Save** um die Konfiguration zu speichern.

Klicken Sie auf **Save** um die Plattformeinstellung zu speichern. Auswählen **Deploy**, wählen Sie die FTD-Einheit aus, auf die Sie die Änderungen anwenden möchten, und klicken Sie auf **Deploy** um mit der Bereitstellung der Plattformeinstellung zu beginnen.

## E-Mail-Einrichtung für Protokollierung

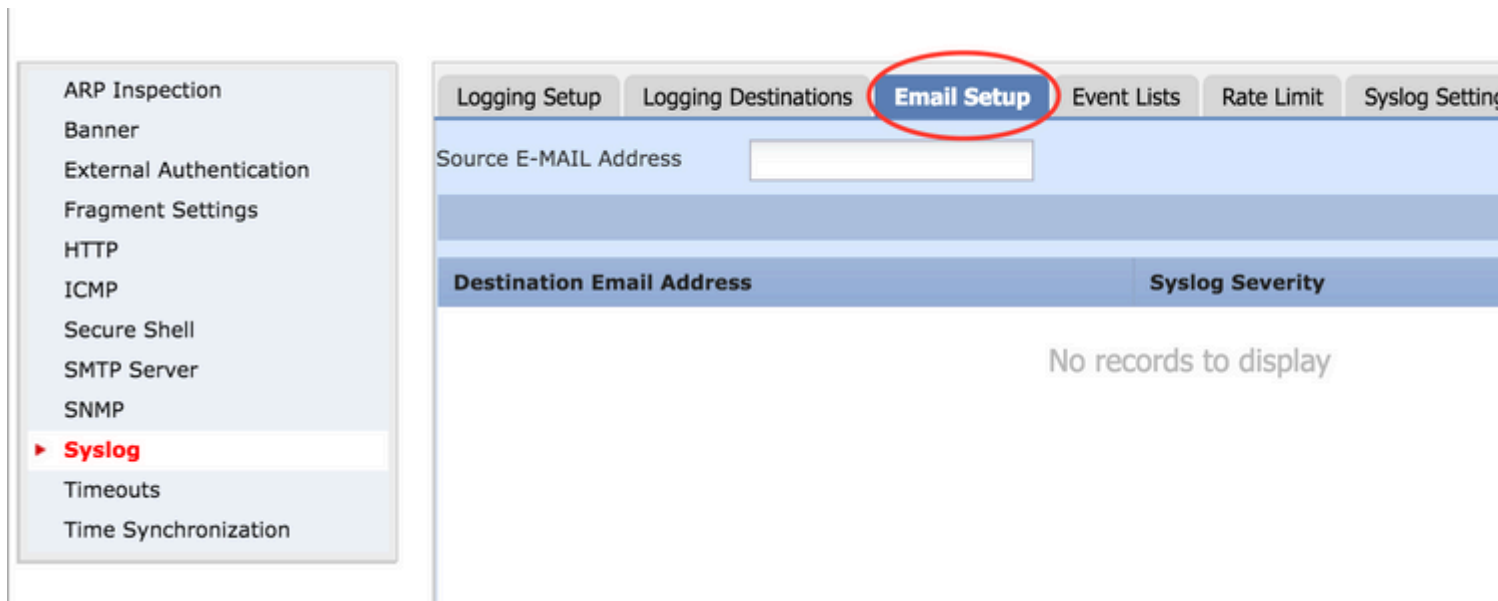
FTD ermöglicht Ihnen, das Syslog an eine bestimmte E-Mail-Adresse zu senden. E-Mail kann nur dann als Protokollierungsziel verwendet werden, wenn bereits ein E-Mail-Relay-Server konfiguriert wurde.

Es gibt zwei Schritte, um E-Mail-Einstellungen für die Syslogs zu konfigurieren.

Schritt 1: Auswählen **Device > Platform Setting > Threat Defense Policy > Syslog > Email Setup**.

Source E-MAIL Address: Geben Sie die Quell-E-Mail-Adresse ein, die in allen aus der FTD versendeten E-Mails

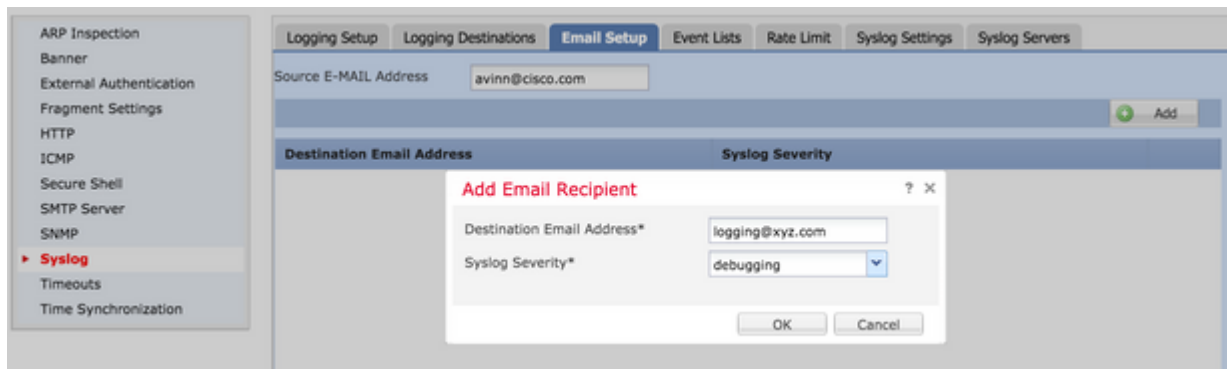
angezeigt wird, die die Syslogs enthalten.



Schritt 2: Um die Ziel-E-Mail-Adresse und den Syslog-Schweregrad zu konfigurieren, klicken Sie auf **Add**.

Destination Email Address: Geben Sie die Ziel-E-Mail-Adresse ein, an die die Syslog-Meldungen gesendet werden.

Syslog Severity: Wählen Sie den Syslog-Schweregrad aus dem **Syslog Severity** aus.



Klicken Sie auf **OK** um die Konfiguration zu speichern.

Klicken Sie auf **save** um die Plattformeinstellung zu speichern. Auswählen **Deploy**, wählen Sie die FTD-Einheit aus, auf die Sie die Änderungen anwenden möchten, und klicken Sie auf **Deploy** um mit der Bereitstellung der Plattformeinstellung zu beginnen.

## Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

## Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

- Überprüfen der FTD-Syslog-Konfiguration in der FTD-CLI Melden Sie sich bei der

Verwaltungsschnittstelle des FTD an, und geben Sie den `system support diagnostic-cli`, um in die Diagnose-CLI zu gelangen.

```
> 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
```

- Stellen Sie sicher, dass der Syslog-Server über FTD erreichbar ist. Melden Sie sich über SSH bei der FTD-Verwaltungsschnittstelle an, und überprüfen Sie die Verbindung mit dem `ping` aus.

```
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
```

- Sie können eine Paketerfassung durchführen, um die Verbindung zwischen dem FTD und dem Syslog-Server zu überprüfen. Melden Sie sich über SSH bei der FTD-Verwaltungsschnittstelle an, und geben Sie den Befehl `system support diagnostic-cli`. Informationen zu den Paketerfassungsbefehlen finden Sie unter [ASA-Paketerfassungen mit CLI und ASDM - Konfigurationsbeispiel](#).
- Stellen Sie sicher, dass die Richtlinienbereitstellung erfolgreich angewendet wird.

## Zugehörige Informationen

- [Cisco Firepower Threat Defense - Kurzreferenz für die ASA](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

## 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.