# Konfigurieren der Anmeldung bei FTD über FMC

## Inhalt



## Einleitung

Dieses Dokument beschreibt die Protokollierungskonfiguration für eine FirePOWER Threat Defense (FTD) über FirePOWER Management Center (FMC).

## Voraussetzungen

### Anforderungen

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

- FirePOWER-Technologie
- Grundkenntnisse der 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 Software-Version 6.0.1 und höher

- ASA FirePOWER Threat Defense-Image für ASA (5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X, ASA 5585-X) mit Software-Version 6.0.1 und höher
- FMC Version 6.0.1 oder 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 verstehen.

## Hintergrundinformationen

Die FTD-Systemprotokolle liefern Ihnen die Informationen zur Überwachung und Fehlerbehebung der FTD-Appliance. Die Protokolle sind sowohl bei der routinemäßigen Fehlerbehebung als auch bei der Incident Behandlung nützlich. Die FTD-Appliance unterstützt sowohl die lokale als auch die externe Protokollierung.

Lokale Protokollierung kann Ihnen bei der Fehlerbehebung helfen. Die externe Protokollierung ist eine Methode zur Erfassung von Protokollen von der FTD-Appliance zu einem externen Syslog-Server. Die Protokollierung bei einem zentralen Server hilft bei der Aggregation von Protokollen und Warnmeldungen. Die externe Protokollierung kann bei der Protokollkorrelation und beim Umgang mit Vorfällen hilfreich sein.

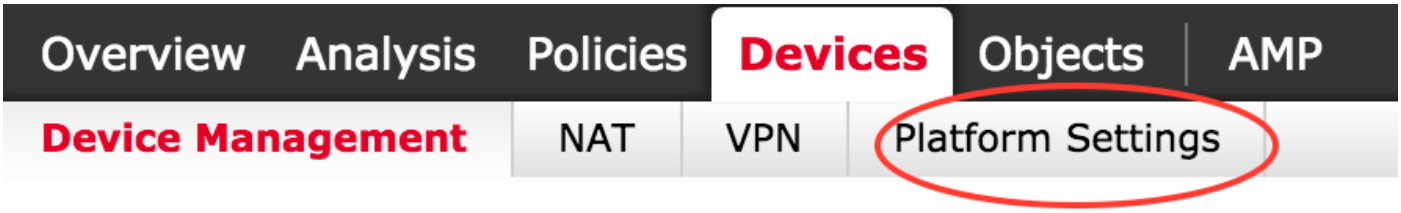
Für die lokale Protokollierung unterstützt die FTD-Appliance die Konsolen- und interne Pufferoption sowie die SSH-Sitzungsprotokollierung (Secure Shell).

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

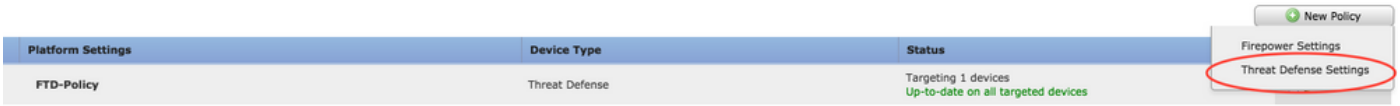
> **Anmerkung:** Wenn ein hohes Datenverkehrsvolumen durch die Appliance geleitet wird, achten Sie auf die Art der Protokollierung/Schweregrad-/Ratenbegrenzung. Führen Sie diese Schritte aus, um die Anzahl der Protokolle zu begrenzen, wodurch die Auswirkungen auf die Firewall vermieden werden.

## Konfigurieren

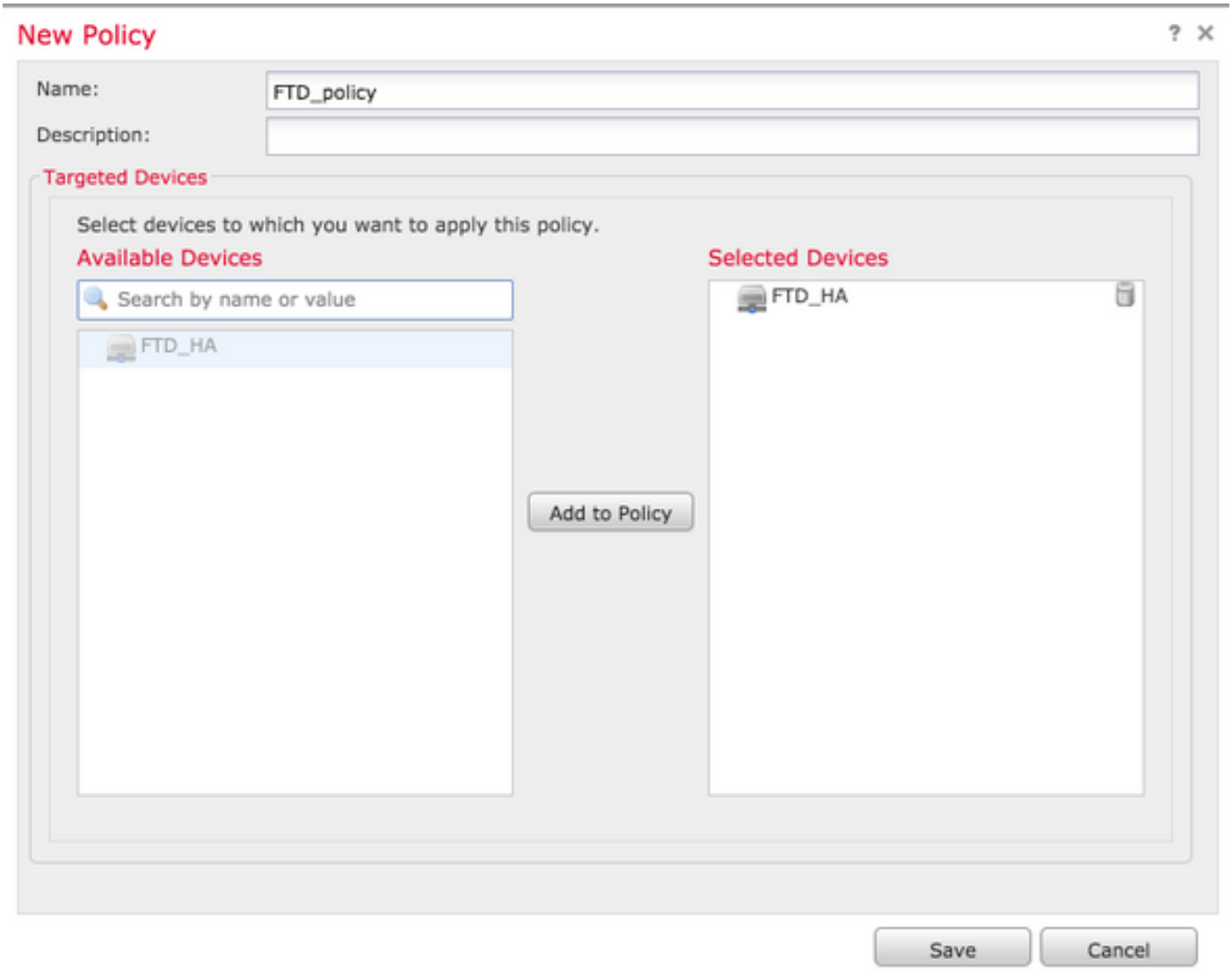
Alle protokollbezogenen Konfigurationen können konfiguriert werden, wenn Sie zum Platform Settings Registerkarte unter Devices Registerkarte. Auswählen Devices > Platform Settings wie in diesem Bild gezeigt.




Klicken Sie entweder 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.




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




## Globale Syslog-Konfiguration konfigurieren

Es gibt bestimmte Konfigurationen, die sowohl für die lokale als auch die externe Protokollierung gelten. In diesem Abschnitt werden die obligatorischen und optionalen Parameter beschrieben, die für Syslog konfiguriert werden können.

### Protokollierung einrichten

Die Protokollierungs-Setup-Optionen gelten für die lokale und die externe Protokollierung. Um die Protokollierungseinrichtung zu konfigurieren, wählen Sie **Devices > Platform Settings**.

Auswählen **Syslog > Logging Setup**.

### Grundlegende Protokollierungseinrichtung

- Enable Logging: Überprüfen Sie die **Enable Logging** aktivieren, 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** aktivieren, um die Protokollierung auf dem Standby-FTD zu konfigurieren, das Teil eines FTD-Hochverfügbarkeitsclusters ist.
- Send syslogs in EMBLEM format: Überprüfen Sie die **Send syslogs in EMBLEM format** aktivieren, 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 Syslog-Format der Cisco IOS Software, das von den Routern und Switches erstellt wurde. Es ist nur für UDP Syslog-Server verfügbar.
- Send debug messages as syslogs: Überprüfen Sie die **Send debug messages as syslogs** aktivieren, 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)

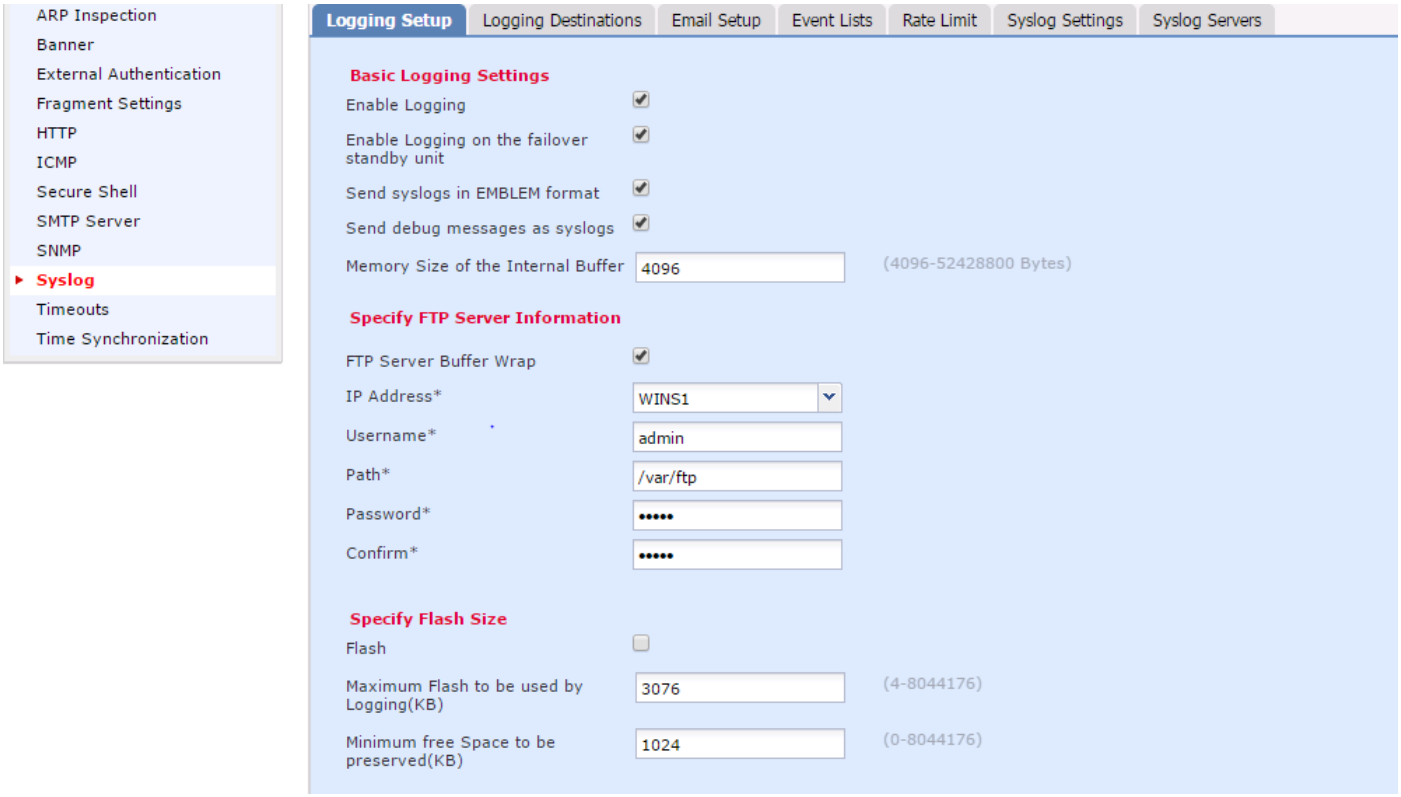
Geben Sie die FTP-Serverdetails an, wenn die Protokolldaten an den FTP-Server gesendet werden sollen, bevor der interne Puffer überschrieben wird.

- FTP Server Buffer Wrap: Überprüfen Sie die **FTP Server Buffer Wrap** aktivieren, 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 im Flash-Speicher speichern möchten, sobald der interne Puffer voll ist.

- Flash: Überprüfen Sie die **Flash** aktivieren, 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 zu bewahrenden Flash-Speichers in KB ein.




Klicken Sie auf **Save** um die Plattformeinstellung zu speichern. Wählen Sie **Deploy** die FTD-Appliance aus, auf die die Änderungen angewendet werden sollen, und klicken Sie auf **Deploy** um die Bereitstellung der Plattformeinstellung zu starten.

## 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 Protokollierungsfilter unter Protokollierungsziele konfigurieren.

Das System ermöglicht zwei Optionen, die Funktionalität benutzerdefinierter Ereignislisten zu verwenden.

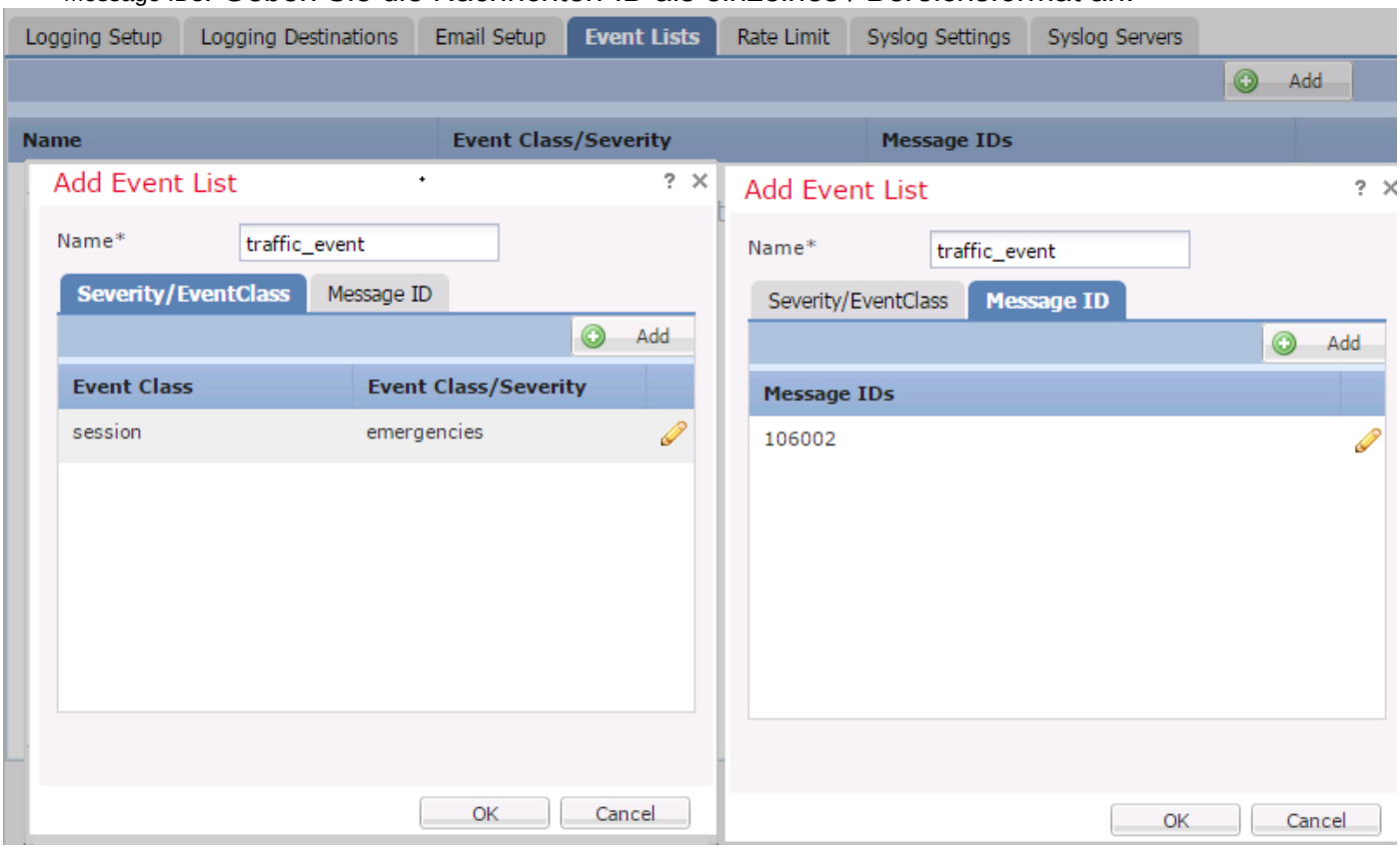
- Klasse und Schweregrad
- Nachrichten-ID

Um benutzerdefinierte Ereignislisten zu konfigurieren, wählen Sie **Device > Platform Setting > Threat Defense Policy > Syslog > Event List** und klicken Sie 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 Typ der Protokolldaten aus, die Sie speichern möchten. Eine Ereignisklasse definiert einen Satz von Syslog-Regeln, die dieselben Funktionen darstellen. Beispielsweise gibt es 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 gewählte Event Class aus. Der Schweregrad kann zwischen 0 (Notfall) und 7 (Debuggen) liegen.
- Message ID: Wenn Sie an spezifischen Protokolldaten zu einer Nachrichten-ID interessiert sind,

klicken Sie auf **Add** um einen Filter auf Basis der Nachrichten-ID einzustellen.

- Message IDs: Geben Sie die Nachrichten-ID als einzelnes / Bereichsformat an.




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

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 die Bereitstellung der Plattformeinstellung zu starten.

### Durchsatzbegrenzendes Syslog

Die Option "Rate limit" definiert die Anzahl der Nachrichten, die an alle konfigurierten Ziele gesendet werden können, und definiert den Schweregrad der Nachricht, der Sie Ratenbeschränkungen zuweisen möchten.

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

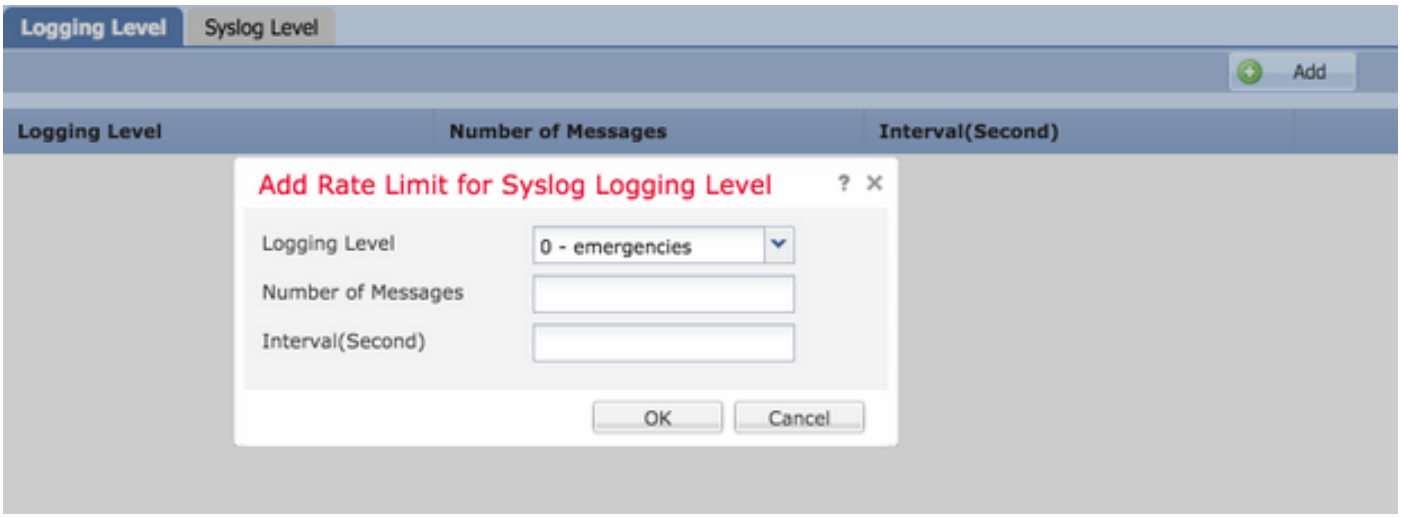
- Protokollierende Stufe
- Syslog-Ebenen

Um die Protokollierungsebenenratenlimit zu aktivieren, wählen Sie **Logging Level** und klicken Sie auf **Add**.

- Logging Level: Von der **Logging Level** aus, wählen Sie die Protokollierungsebene aus, für die Sie die Ratenbegrenzung durchführen möchten.
- Number of Messages: Geben Sie die maximale Anzahl an Syslog-Meldungen ein, die innerhalb des angegebenen Intervalls empfangen werden sollen.
- Interval(Second): Geben Sie auf Basis des Parameters Number of Messages (Anzahl der

Nachrichten), der zuvor konfiguriert wurde, das Zeitintervall ein, in dem eine Reihe von Syslog-Meldungen empfangen werden können.

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

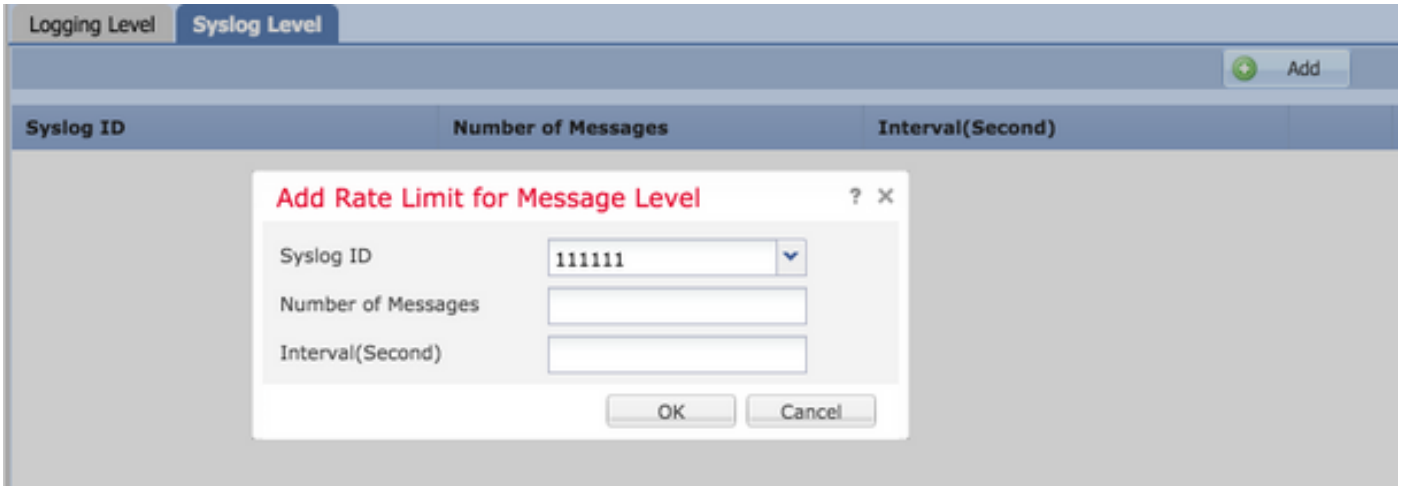



Klicken Sie auf **OK** um die Konfiguration der Protokollierungsebene zu speichern.

Um das Protokollierungsebenenlimit zu aktivieren, wählen Sie **Logging Level** und klicken Sie auf **Add**.

- Syslog ID: Syslog-IDs werden zur eindeutigen Identifizierung der Syslog-Meldungen verwendet. Von der **Syslog ID** aus, wählen Sie die Syslog-ID aus.
- Number of Messages: Geben Sie die maximale Anzahl an Syslog-Meldungen ein, die innerhalb des angegebenen Intervalls empfangen werden sollen.
- Interval(Second): Geben Sie auf Basis des Parameters Number of Messages (Anzahl der Nachrichten), der zuvor konfiguriert wurde, das Zeitintervall ein, in dem eine Reihe von Syslog-Meldungen empfangen werden können.

Die Syslog-Geschwindigkeit entspricht der Anzahl der Nachrichten/des Intervalls.




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

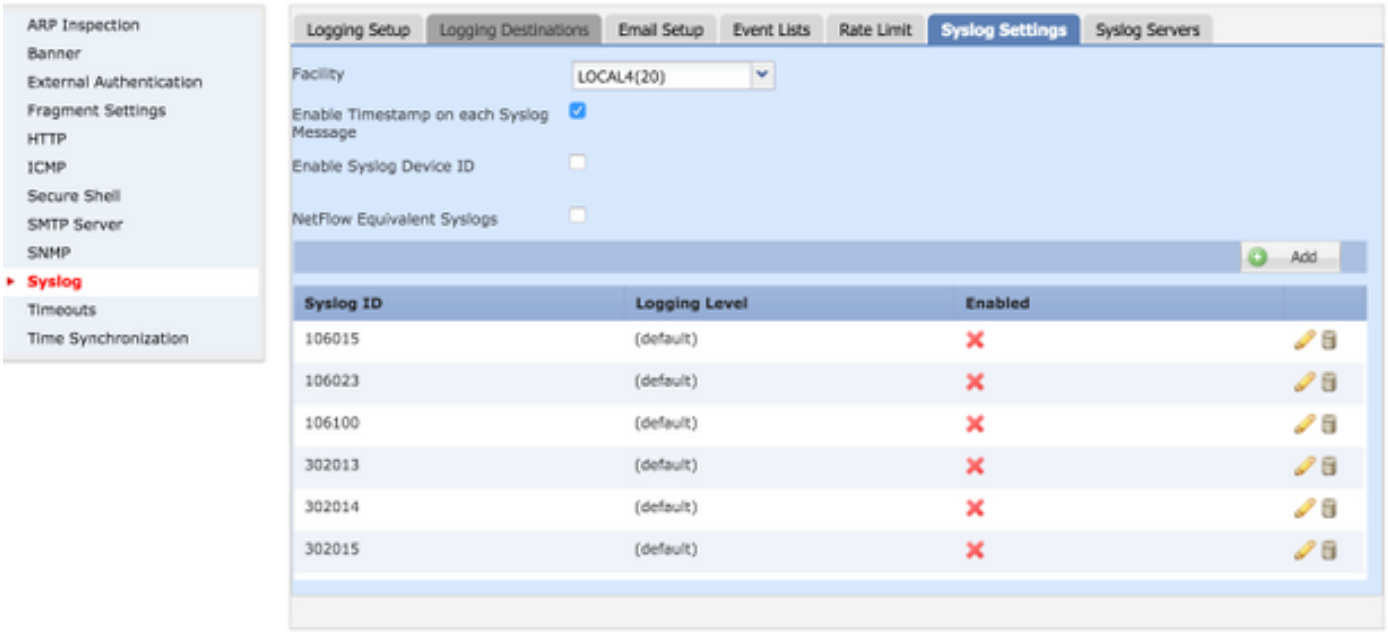
Klicken Sie auf **Save** um die Plattformeinstellung zu speichern. Wählen Sie **Deploy**, wählen Sie die FTD-Appliance aus, auf die Sie die Änderungen anwenden möchten, und klicken Sie auf **Deploy** um die Bereitstellung der Plattformeinstellung zu starten.

### Syslog-Einstellungen

Mithilfe der Syslog-Einstellungen kann die Konfiguration der Anlagenwerte in die Syslog-Meldungen aufgenommen werden. Sie können den Zeitstempel auch in Protokollmeldungen und andere serverspezifische Syslog-Parameter einschließen.

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

- Facility: Ein Funktionscode wird verwendet, um den Programmtyp anzugeben, der die Nachricht protokolliert. Nachrichten mit unterschiedlichen Einrichtungen können unterschiedlich behandelt werden. Von der **Facility** aus, wählen Sie den Wert für die Einrichtung aus.
- Enable Timestamp on each Syslog Message: Überprüfen Sie die **Enable Timestamp on each Syslog Message** aktivieren, um den Zeitstempel in Syslog-Meldungen einzufügen.
- Enable Syslog Device ID: Überprüfen Sie die **Enable Syslog Device ID** aktivieren, um eine Geräte-ID in Syslog-Meldungen im Nicht-EMBLEM-Format einzuschließen.
- Netflow Equivalent Syslogs: Überprüfen Sie die **Netflow Equivalent Syslogs** aktivieren, um NetFlow-entsprechende 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 geben Sie Folgendes an: **Syslog ID/ Logging Level** aktivieren.




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 die Bereitstellung der Plattformeinstellung zu starten.

## Lokale Protokollierung konfigurieren

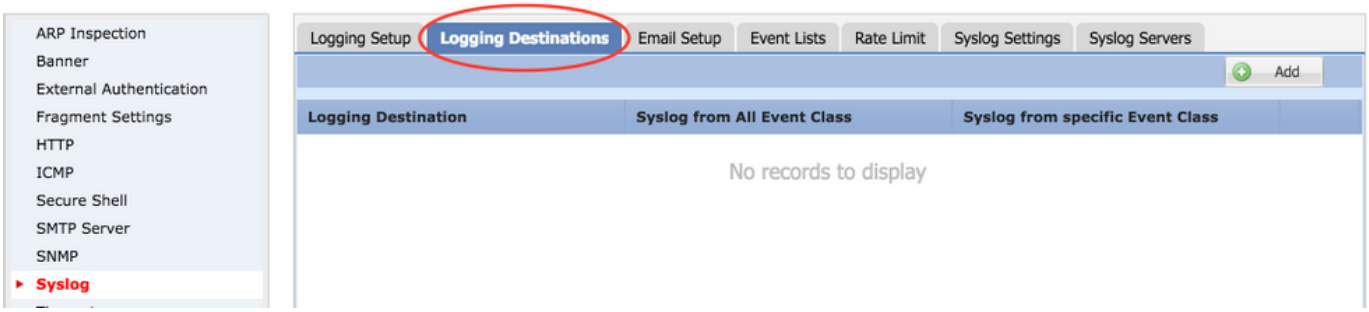
Der Abschnitt "Logging Destination" (Anmeldename-Ziel) kann verwendet werden, um die Protokollierung für bestimmte Ziele zu konfigurieren.

Die verfügbaren internen Protokollierungsziele sind:

- Interner Puffer: Protokolle am internen Protokollierungspuffer (gepufferte Protokollierung)
- Konsole: Sendet Protokolle an die Konsole (Protokollkonsole)
- SSH-Sitzungen: Protokolliert Syslog bei SSH-Sitzungen (Terminalmonitor)

Die lokale Protokollierung kann in drei Schritten konfiguriert werden.

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



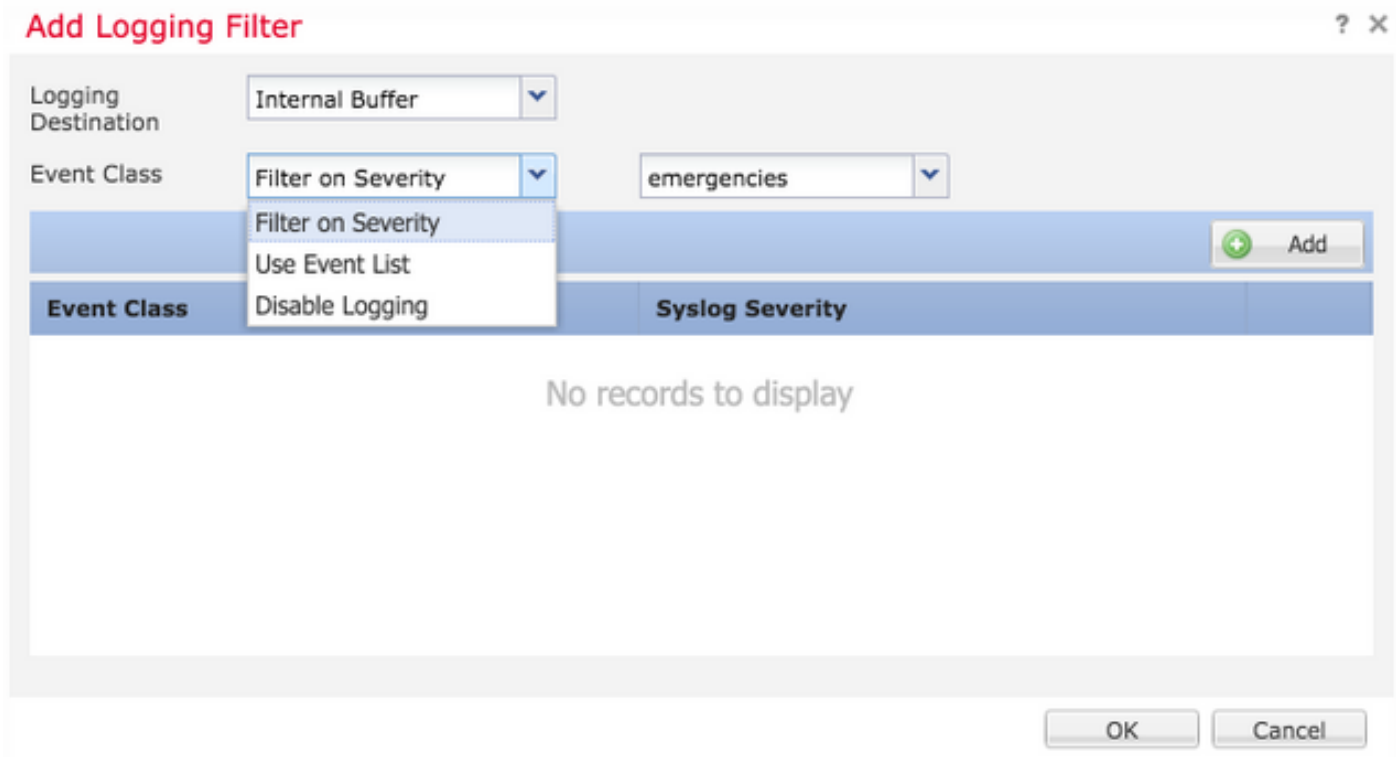

Schritt 2: Klicken Sie auf **Add** um einen Protokollfilter für eine bestimmte **logging destination.**

Protokollierungsziel: Wählen Sie das gewünschte Protokollierungsziel aus dem **Logging Destination** als interne Puffer-, Konsolen- oder SSH-Sitzungen angezeigt.

Ereignisklasse: Von der **Event Class** aus, wählen Sie eine Event-Klasse aus. Wie bereits beschrieben, sind Ereignisklassen eine Gruppe von Syslogs, die die gleichen Funktionen darstellen. Ereignisklassen können folgendermaßen ausgewählt werden:

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

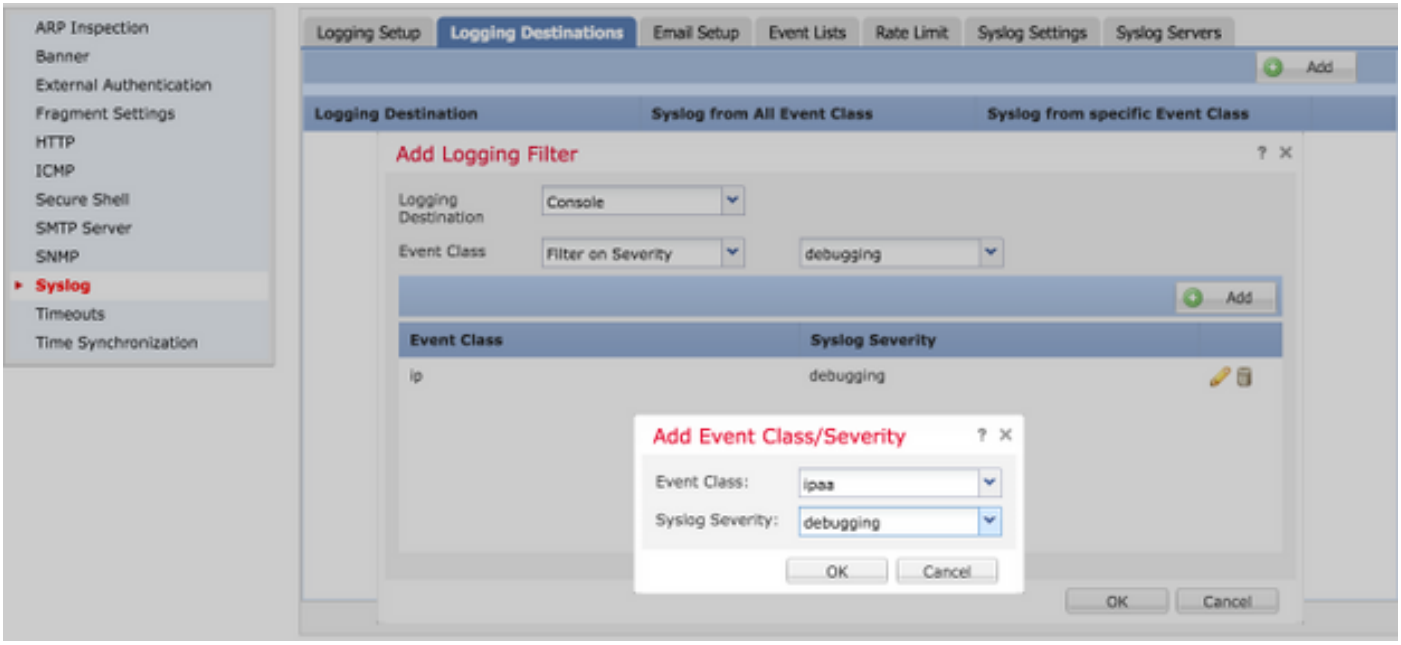
Protokollierende Stufe: Wählen Sie die Protokollierungsebene aus der Dropdown-Liste aus. Der Bereich der Protokollierungsebene reicht von 0 (Notfälle) bis 7 (Debuggen).




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

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

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




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

Klicken Sie auf **Save** um die Plattformeinstellung zu speichern. Auswählen **Deploy**, wählen Sie die FTD-Appliance aus, auf die Sie die Änderungen anwenden möchten, und klicken Sie auf **Deploy** um die Bereitstellung 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 Art der externen Protokollierung.

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

Die Konfiguration für die externe Protokollierung und die interne Protokollierung ist identisch. Die Auswahl der Protokollierungsziele bestimmt die Art der implementierten Protokollierung. Es ist möglich, Ereignisklassen auf der Grundlage von benutzerdefinierten Ereignislisten für den Remoteserver zu konfigurieren.

### Remote-Syslog-Server

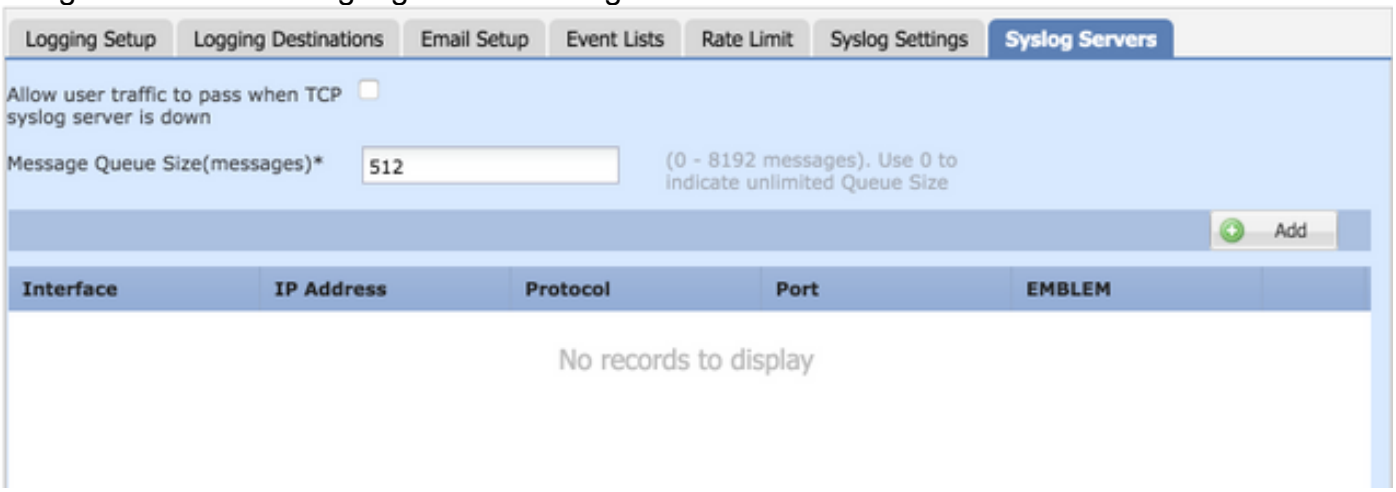
Syslog-Server können so konfiguriert werden, dass sie Protokolle remote von der FTD aus analysieren und speichern.

Es gibt drei Schritte zur Konfiguration von Syslog-Remote-Servern.

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

Schritt 2: Konfigurieren Sie den Parameter für den Syslog-Server.

- Zulassen, dass Benutzerdatenverkehr weitergeleitet wird, wenn der TCP-Syslog-Server ausgefallen ist: Wenn im Netzwerk ein TCP-Syslog-Server bereitgestellt wurde und dieser nicht erreichbar ist, wird der Netzwerkverkehr über die ASA abgelehnt. Dies gilt nur, wenn das Transportprotokoll zwischen ASA und dem Syslog-Server TCP ist. Überprüfen Sie die **Allow user traffic to pass when TCP syslog server is down** aktivieren, damit Datenverkehr die Schnittstelle passieren kann, wenn der Syslog-Server ausgefallen ist.
- Nachrichtenwarteschlangengröße: Die Nachrichtenwarteschlangengröße ist die Anzahl der Meldungen, die im FTD in die Warteschlange gestellt werden, wenn der Remote-Syslog-Server belegt ist und keine Protokollmeldungen akzeptiert. Der Standardwert ist 512 Nachrichten, und die Mindestgröße ist 1 Nachricht. Wenn in dieser Option 0 angegeben ist, gilt die Warteschlangengröße als unbegrenzt.




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

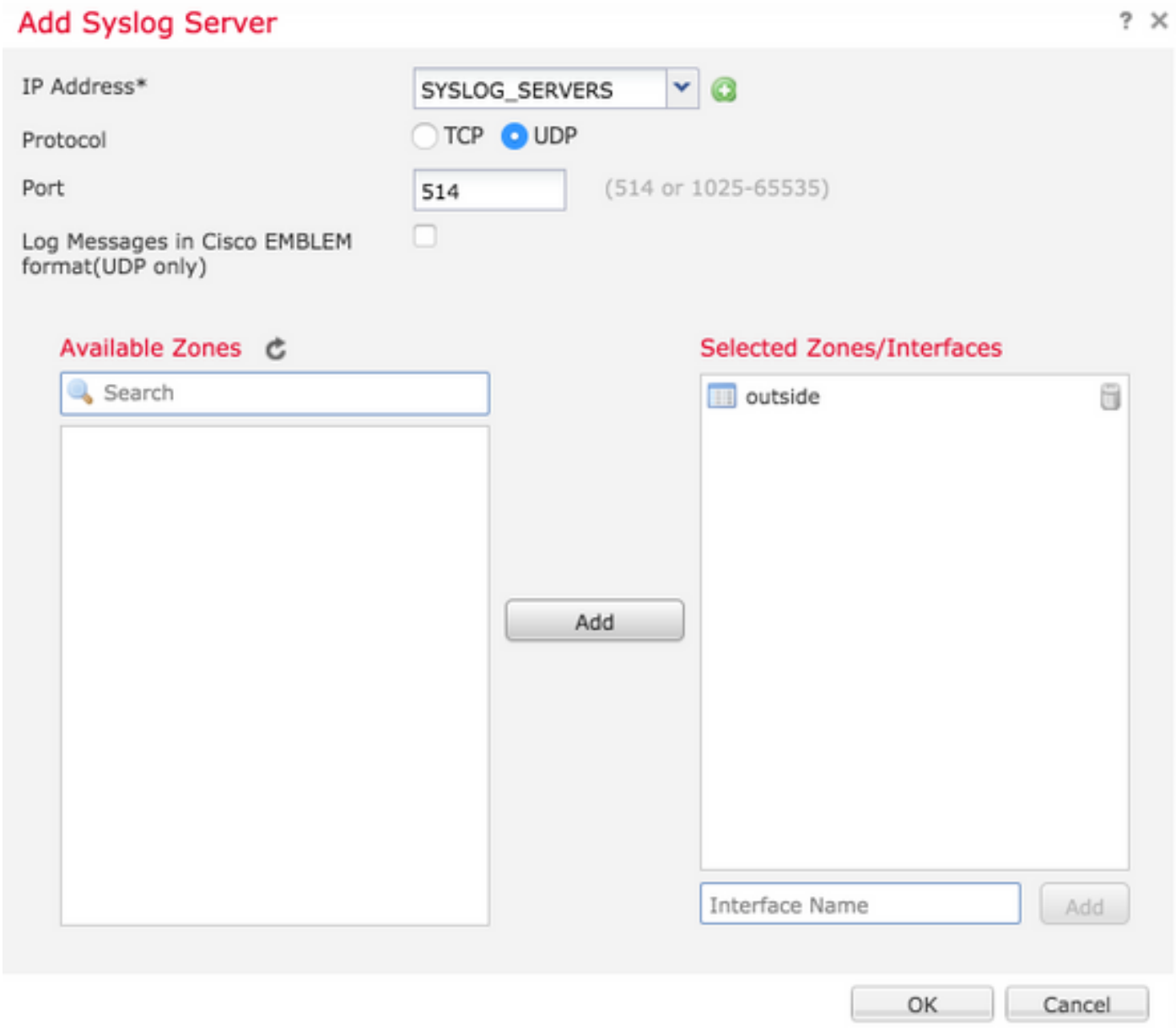
IP Address: Von der **IP Address** aus, wählen Sie ein Netzwerkobjekt aus, in dem die Syslog-Server aufgeführt sind. Wenn Sie noch kein Netzwerkobjekt erstellt haben, klicken Sie auf das Pluszeichen (+), um ein neues Objekt zu erstellen.

Protocol: Klicken Sie entweder auf **TCP** Oder **UDP** 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 Nachrichten im Cisco EMBLEM-Format protokolliert werden sollen. Dies gilt nur für UDP-basiertes 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.




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-Appliance aus, auf die Sie die Änderungen anwenden möchten, und klicken Sie auf **Deploy** um die Bereitstellung der Plattformeinstellung zu starten.

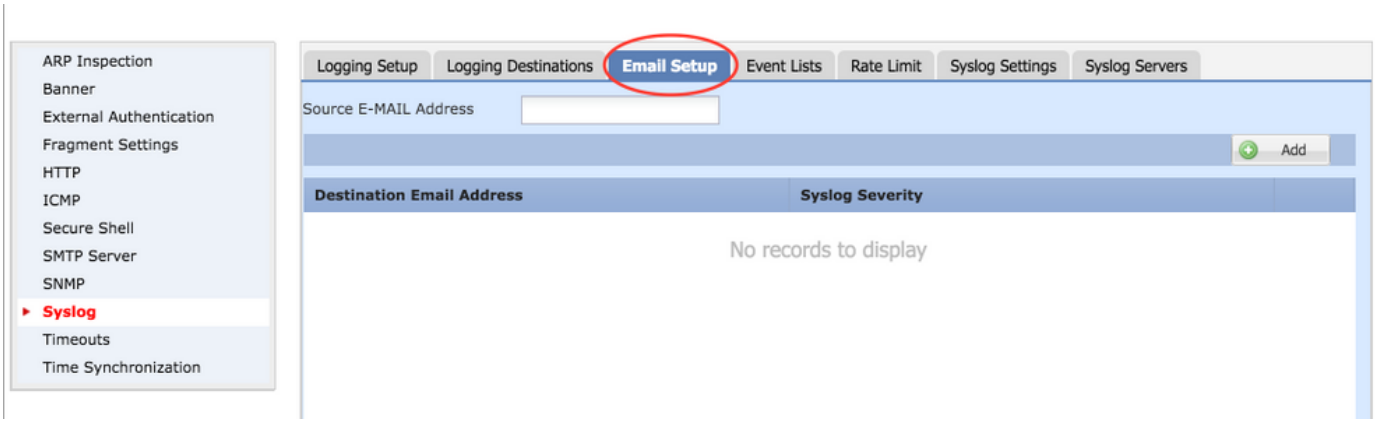
### E-Mail-Setup für die Protokollierung

Mit FTD können Sie das Syslog an eine bestimmte E-Mail-Adresse senden. E-Mails können nur dann als Protokollierungsziel verwendet werden, wenn bereits ein E-Mail-Relay-Server konfiguriert wurde.

Es gibt zwei Schritte zum Konfigurieren der E-Mail-Einstellungen für die Syslogs.

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

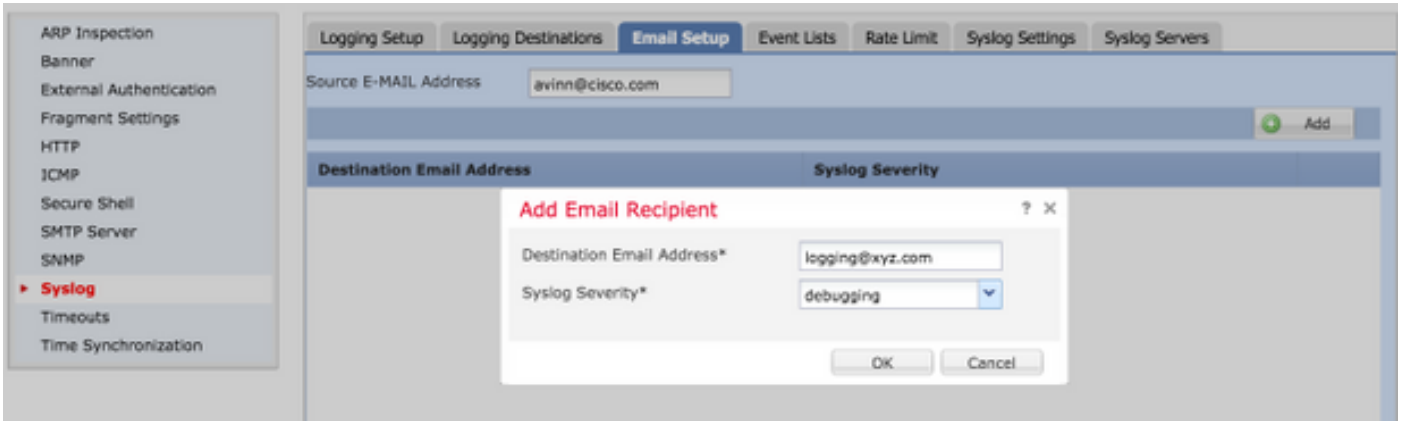
Source E-MAIL Address: Geben Sie die Quell-E-Mail-Adresse ein, die auf allen E-Mails angezeigt wird, die von der FTD gesendet wurden und die Syslogs enthalten.




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-Appliance aus, auf die Sie die Änderungen anwenden möchten, und klicken Sie auf **Deploy** um die Bereitstellung der Plattformeinstellung zu starten.

# Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

# Fehlerbehebung

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

- Überprüfen Sie die FTD-Syslog-Konfiguration in der FTD-CLI. Melden Sie sich bei der Verwaltungsschnittstelle des FTD an, und geben Sie die **system support diagnostic-cli** , um die Konsole in die Diagnose-CLI zu übernehmen.

```
> 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 von der FTD aus erreichbar ist. Melden Sie sich über SSH bei der FTD-Managementschnittstelle 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-Managementschnittstelle an, und geben Sie den Befehl ein. **system support diagnostic-cli**. Die Befehle zur Paketerfassung finden Sie unter ASA Packet Captures with CLI and ASDM Configuration Example.
- Stellen Sie sicher, dass die Richtlinienbereitstellung erfolgreich angewendet wird.

# Zugehörige Informationen

- Cisco FirePOWER Threat Defense - Kurzanleitung für die ASA
- Technischer Support und Dokumentation für Cisco Systeme