

Logboekregistratie configureren op FTD via FMC

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Globale systeemconfiguratie configureren](#)

[Logboekregistratie](#)

[Lijsten van gebeurtenissen](#)

[Snelheidsbeperking voor syslog](#)

[Syslog-instellingen](#)

[Lokale vastlegging configureren](#)

[Het externe vastlegging configureren](#)

[Remote System-server](#)

[E-mail instellen voor vastlegging](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt de configuratie van logboekregistratie voor Firepower Threat Defense (FTD) via Firepower Management Center (FMC) beschreven.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- FirePOWER-technologie
- Adaptieve security applicatie (ASA)
- Syslog-protocol

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASA Firepower Threat Defence Image voor ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) waarop softwareversie 6.0.1 en hoger wordt uitgevoerd
- ASA Firepower Threat Defence Image voor ASA (5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) waarop softwareversie 6.0.1 en hoger wordt uitgevoerd
- VCC, versie 6.0.1 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als

uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De FTD-systeemlogboeken bieden u de informatie om het FTD-apparaat te bewaken en probleemoplossing te bieden.

De logboeken zijn nuttig zowel bij het routinematig oplossen van problemen als bij de incidentele behandeling. Het FTD-apparaat ondersteunt zowel lokale als externe logboekregistratie.

Lokale logboekregistratie kan u helpen bij het oplossen van de live problemen. Externe logboekregistratie is een methode voor het verzamelen van logbestanden van het FTD-apparaat naar een externe Syslog-server.

Vastlegging op een centrale server helpt bij het samenvoegen van logbestanden en waarschuwingen. Externe logboekregistratie kan helpen bij logcorrelatie en incidentafhandeling.

Voor lokale logboekregistratie ondersteunt het FTD-apparaat console, interne bufferoptie en de logboekregistratie voor Secure Shell (SSH).

Voor externe logboekregistratie ondersteunt het FTD-apparaat de externe Syslog-server en de E-mail Relay-server.

Opmerking: als er veel verkeer door het apparaat komt, let dan op het type logboekregistratie/de beperking van de ernst/snelheid. Doe dit om het aantal logbestanden te beperken, waardoor de impact op de firewall wordt vermeden.

Configureren

Alle met vastlegging verband houdende configuraties kunnen worden geconfigureerd wanneer u naar de Platform Settings tabblad onder de Devices tabblad. Kiezen Devices > Platform Settings zoals in deze afbeelding.



Klik op het pictogram om het bestaande beleid te bewerken of klik op New Policyen kies vervolgens Threat Defense Settings om een nieuw FTD-beleid te creëren zoals in deze afbeelding wordt getoond.

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

Selecteer het FTD-apparaat om dit beleid toe te passen en klik op Save zoals in deze afbeelding.

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

Globale systeemconfiguratie configureren

Er zijn bepaalde configuraties die van toepassing zijn voor zowel lokale als externe logboekregistratie. Dit deel gaat over de verplichte en optionele parameters die voor Syslog kunnen worden geconfigureerd.

Logboekregistratie

De instellopties voor vastlegging zijn van toepassing voor lokale en externe vastlegging. Kies deze optie om de loginstelling te configureren **Devices > Platform Settings**.

Kiezen Syslog > **Logging Setup**.

Basis vastlegging

- **Enable Logging:** Controleer de **Enable Logging** vink dit selectievakje aan om de logboekregistratie in te schakelen. Dit is een verplichte optie.
- **Enable Logging on the failover standby unit:** Controleer de **Enable Logging on the failover standby unit** vink dit selectievakje aan om het inloggen te configureren op het standby FTD dat deel uitmaakt van een FTD High Availability-cluster.
- **Send syslogs in EMBLEM format:** Controleer de **Send syslogs in EMBLEM format** Schakel dit selectievakje in om het formaat Syslog als EMBLEM voor elke bestemming in te schakelen. Het EMBLEM-formaat wordt voornamelijk gebruikt voor de CiscoWorks Resource Manager Essentials (RME) Syslog-analyzer. Dit formaat komt overeen met het formaat Cisco IOS-software synchrone dat door de routers en de switches wordt geproduceerd. Het is alleen beschikbaar voor UDP Syslog-servers.
- **Send debug messages as syslogs:** Controleer de **Send debug messages as syslogs** Schakel dit selectievakje in om de debug-logbestanden als Syslog-berichten naar de Syslog-server te versturen.
- **Memory size of the Internal Buffer:** Geef de grootte van de interne geheugenbuffer op waar FTD de

loggegevens kan opslaan. De loggegevens worden geroteerd als de bufferlimiet wordt bereikt.

Informatie over FTP-server (optioneel)

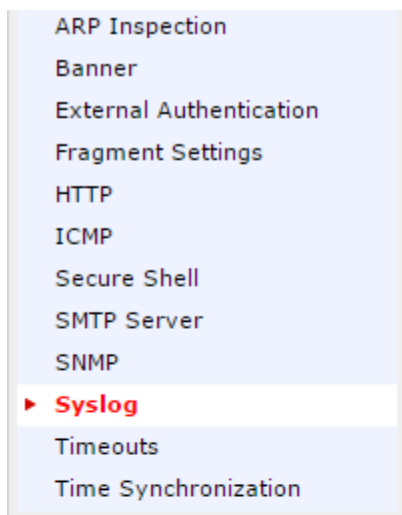
Geef FTP-servergegevens op als u de loggegevens naar FTP-server wilt verzenden voordat de interne buffer wordt overschreven.

- **FTP Server Buffer Wrap:** Controleer de **FTP Server Buffer Wrap** vink dit aan om de bufferloggegevens naar de FTP-server te sturen.
- **IP Address:** Voer het IP-adres van de FTP-server in.
- **Username:** Voer de gebruikersnaam in van de FTP-server.
- **Path:** Voer het directorypad van de FTP-server in.
- **Password:** Voer het wachtwoord van de FTP-server in.
- **Confirm:** Voer hetzelfde wachtwoord opnieuw in.

Flitsformaat (optioneel)

Specificeer de flitsgrootte als u de loggegevens aan flitser wilt opslaan zodra de interne buffer vol is.

- **Flash:** Controleer de **Flash** controlevakje om de loggegevens naar de interne flitser te verzenden.
- **Maximum Flash to be used by Logging(KB):** Voer de maximale grootte in kB van het flitsgeheugen in dat voor het vastleggen kan worden gebruikt.
- **Minimum free Space to be preserved(KB):** Voer de minimumgrootte in KB van het flitsgeheugen in dat moet worden bewaard.



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)

Klik op de knop **Save** om de platforminstelling op te slaan. Kies de **Deploy** Kies de FTD-applicatie waar u de wijzigingen wilt toepassen en klik vervolgens op **Deploy** om de invoering van de platforminstelling te starten.

Lijsten van gebeurtenissen

Met de optie Gebeurtenislijsten configureren kunt u een gebeurtenislijst maken/bewerken en opgeven welke loggegevens in het filter van de gebeurtenislijst moeten worden opgenomen. De Lijsten van de gebeurtenis kunnen worden gebruikt wanneer u Filters van het Vastleggen onder de bestemmingen van het Vastleggen vormt.

Het systeem staat twee opties toe om de functionaliteit van de lijsten van de douanegebeurtenis te gebruiken.

- Klasse en ernst
- Bericht-ID

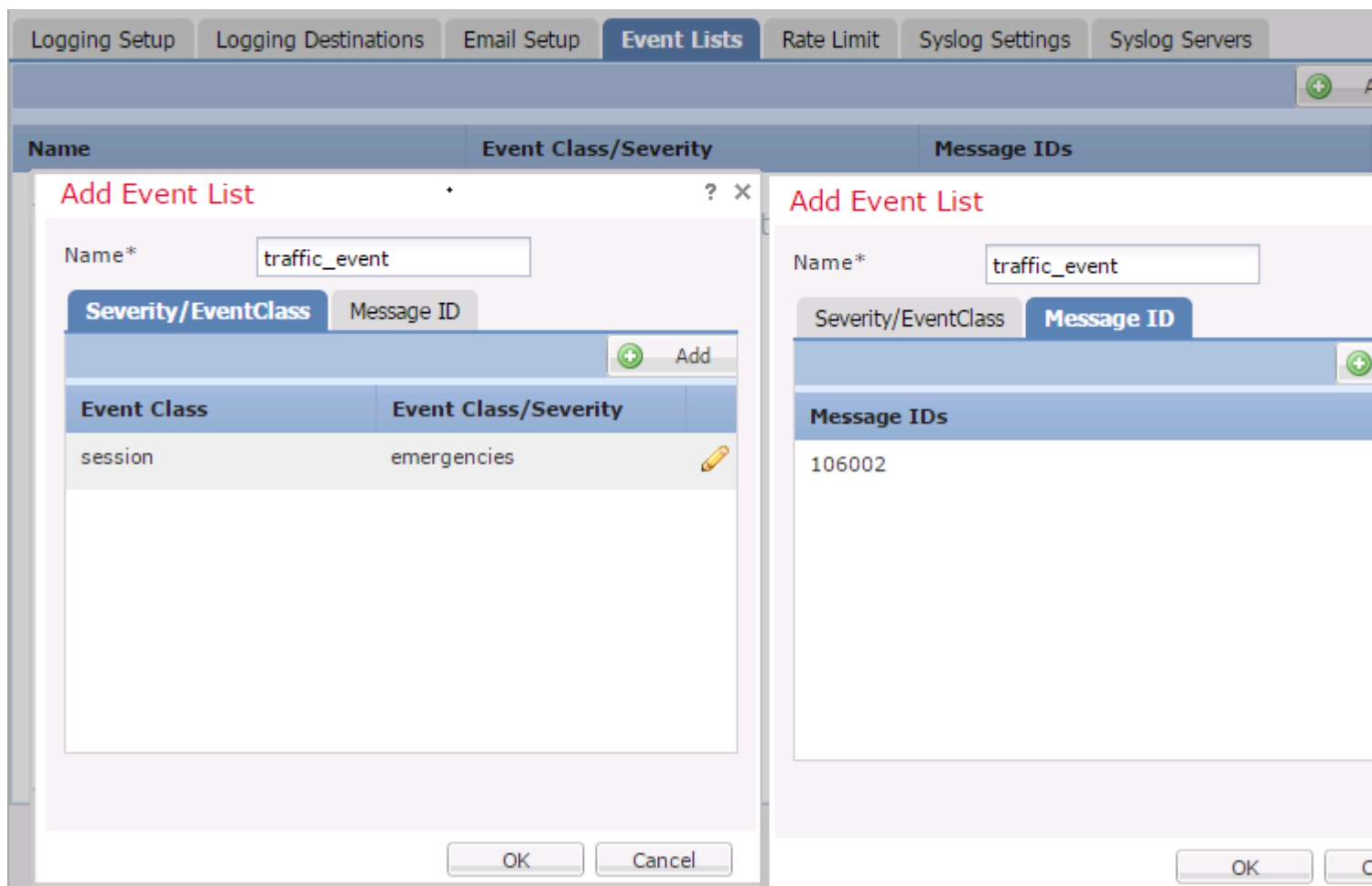
Om de lijsten van de douanegebeurtenis te vormen, kies **Device > Platform Setting > Threat Defense Policy > Syslog > Event List** en klik op **Add**. Dit zijn de opties:

- Name: Voer de naam van de gebeurtenislijst in.
- Severity/Event Class: In het gedeelte Severity/Event Class klikt u op **Add**.
- Event Class: Kies de gebeurtenisklasse in de vervolgkeuzelijst voor het gewenste type loggegevens. Een klasse van de Gebeurtenis bepaalt een reeks regels Syslog die de zelfde eigenschappen

vertegenwoordigen.

Er is bijvoorbeeld een Event Class voor de sessie die alle Syslogs omvat die betrekking hebben op de sessie.

- Syslog Severity: Kies de ernst van de vervolgkeuzelijst voor de gekozen Event Class. De ernst kan variëren van 0 (noodgeval) tot 7 (debugging).
- Message ID: Als u geïnteresseerd bent in specifieke loggegevens met betrekking tot een bericht-ID, klikt u op **Add** om een filter te plaatsen op basis van het bericht-ID.
- Message IDs: Specificeer de bericht-ID als afzonderlijk/bereik-formaat.



Klik op de knop **OK** om de configuratie op te slaan.

Klik op de knop **save** om de platforminstelling op te slaan. Kies voor **Deploy** Kies het FTD-apparaat op de plaats waar u de wijzigingen wilt toepassen en klik op **Deploy** om de invoering van de platforminstelling te starten.

Snelheidsbeperking voor syslog

De snelheidslimietoptie definieert het aantal berichten dat naar alle geconfigureerde bestemmingen kan worden verzonden en definieert de ernst van het bericht waaraan u snelheidslimieten wilt toewijzen.

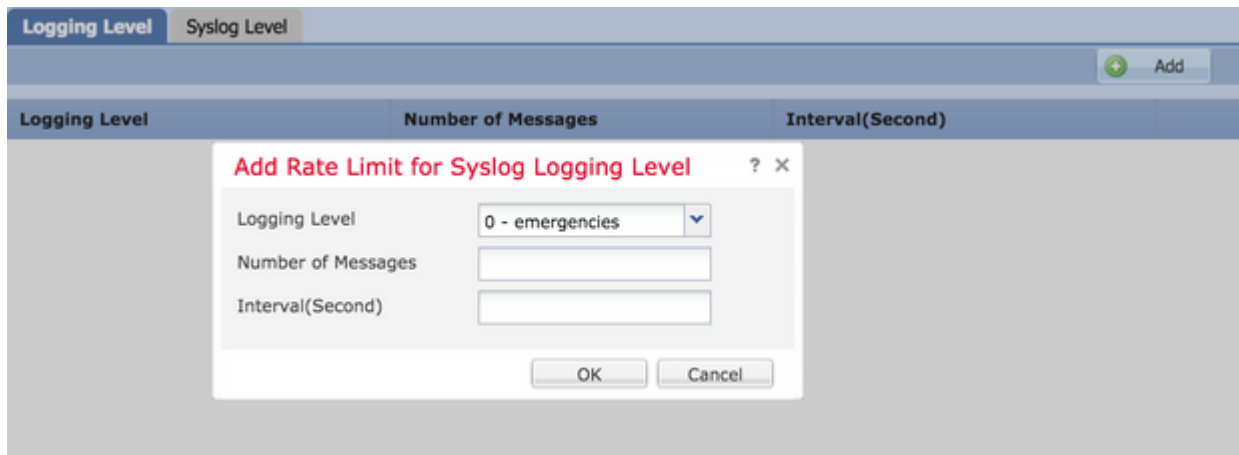
Om de lijsten van de douanegebeurtenis te vormen, kies **Device > Platform Setting > Threat Defense Policy > Syslog > Rate Limit**. U hebt twee opties op basis waarvan u de snelheidslimiet kunt instellen:

- Vastleggingsniveau
- Syslog-niveaus

Om de op registratieniveau gebaseerde snelheidslimiet in te schakelen, kiest u **Logging Level** en klik op **Add**.

- **Logging Level:** van de **Logging Level** Kies het registratieniveau waarvoor u de snelheidsbeperking wilt uitvoeren.
- **Number of Messages:** Voer het maximale aantal Syslog-berichten in dat binnen het opgegeven interval moet worden ontvangen.
- **Interval(Second):** Gebaseerd op de parameter **Number of Messages** die eerder is geconfigureerd, voer het tijdsinterval in waarin een vaste set Syslog-berichten kan worden ontvangen.

Het tarief van Syslog is het Aantal Berichten/intervallen.



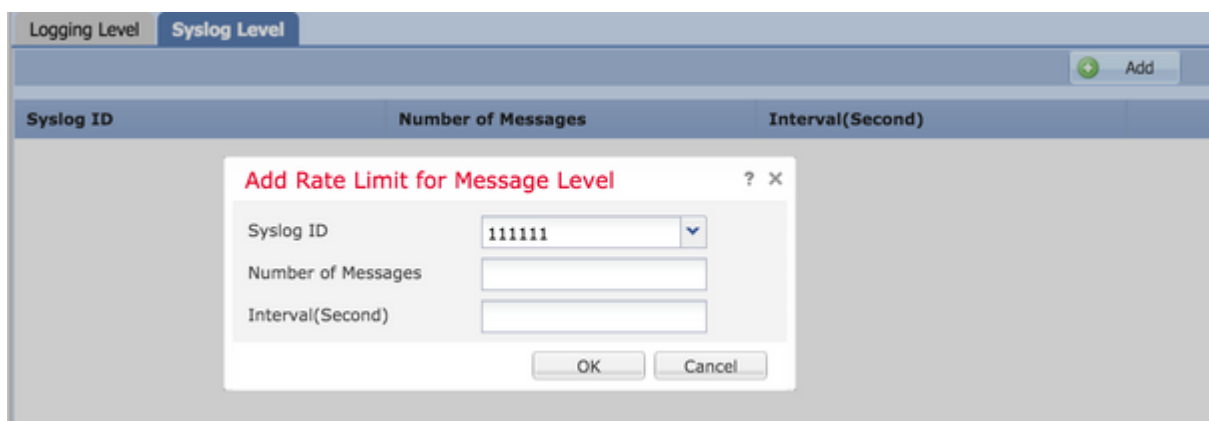
The screenshot shows a web interface with two tabs: 'Logging Level' and 'Syslog Level'. The 'Logging Level' tab is active. Below the tabs is a table with three columns: 'Logging Level', 'Number of Messages', and 'Interval(Second)'. An 'Add' button is in the top right corner. A modal dialog box titled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

Klik op de knop **OK** om de configuratie op registratieniveau op te slaan.

Om de op registratieniveau gebaseerde snelheidslimiet in te schakelen, kiest u **Logging Level** en klik op **Add**.

- **Syslog ID:** Syslog ID's worden gebruikt om de Syslog-berichten uniek te identificeren. Van de **Syslog ID** Kies de Syslog-ID.
- **Number of Messages:** Voer het maximale aantal syslogberichten in dat binnen het opgegeven interval moet worden ontvangen.
- **Interval(Second):** Gebaseerd op de parameter **Number of Messages** die eerder is geconfigureerd, voer het tijdsinterval in waarin een vaste set Syslog-berichten kan worden ontvangen.

Het tarief van Syslog is het Aantal Berichten/Interval.



The screenshot shows a web 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)'. An 'Add' button is in the top right corner. A modal dialog box titled 'Add Rate Limit for Message Level' is open in the center. It contains three input fields: 'Syslog ID' (a dropdown menu showing '111111'), 'Number of Messages' (an empty text box), and 'Interval(Second)' (an empty text box). At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Klik op de knop **OK** om de Syslog-configuratie op te slaan.

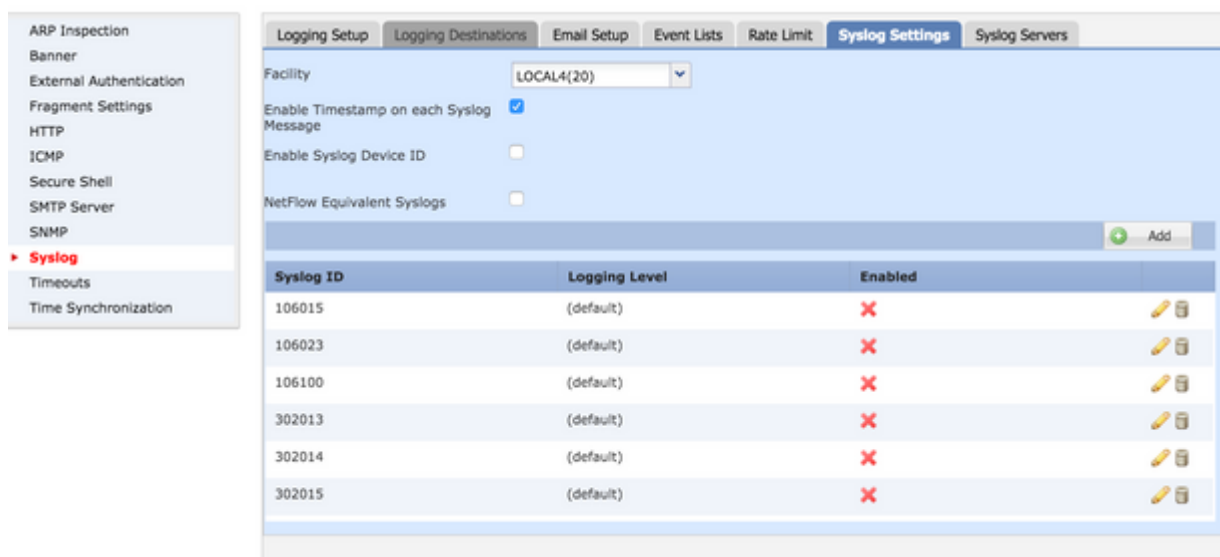
Klik op de knop **Save** om de platforminstelling op te slaan. Kies voor **Deploy** Kies het FTD-apparaat op de plaats waar u de wijzigingen wilt toepassen en klik op **Deploy** om de invoering van de platforminstelling te starten.

Syslog-instellingen













Syslog-instellingen maken het mogelijk de configuratie van de Faciliteitswaarden in de Syslog-berichten op te nemen. U kunt ook de tijdstempel opnemen in logberichten en andere Syslog server-specifieke parameters.

Om de lijsten van de douanegebeurtenis te vormen, kies **Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Settings**.

- **Facility:** Er wordt een faciliteitcode gebruikt om het type programma te specificeren dat het bericht vastlegt. Berichten met verschillende faciliteiten kunnen op verschillende manieren worden verwerkt. Van de **Facility** Vervolgkeuzelijst, kies de faciliteitswaarde.
- **Enable Timestamp on each Syslog Message:** Controleer de **Enable Timestamp on each Syslog Message** vink dit selectievakje aan om de tijdstempel op te nemen in Syslog-berichten.
- **Enable Syslog Device ID:** Controleer de **Enable Syslog Device ID** vink dit selectievakje aan om een apparaat-ID op te nemen in Syslog-berichten zonder EMBLEM-formaat.
- **Netflow Equivalent Syslogs:** Controleer de **Netflow Equivalent Syslogs** vink dit selectievakje aan om NetFlow-equivalente Syslogs te verzenden. Dit kan de prestaties van het apparaat beïnvloeden.
- **Specifieke Syslog-id toevoegen:** om de extra Syslog-id op te geven, klikt u op **Add** en de **Syslog ID/ Logging Level** vink het vakje aan.



The screenshot shows the 'Syslog Settings' configuration page. On the left is a navigation menu with 'Syslog' selected. The main area has tabs for 'Logging Setup', 'Logging Destinations', 'Email Setup', 'Event Lists', 'Rate Limit', 'Syslog Settings', and 'Syslog Servers'. Under 'Syslog Settings', there are options for 'Facility' (set to LOCAL4(20)), 'Enable Timestamp on each Syslog Message' (checked), 'Enable Syslog Device ID' (unchecked), and 'NetFlow Equivalent Syslogs' (unchecked). Below these is an 'Add' button and a table of Syslog IDs.

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

Klik op de knop **Save** om de platforminstelling op te slaan. Kies voor **Deploy** Kies het FTD-apparaat op de plaats waar u de wijzigingen wilt toepassen en klik op **Deploy** om de invoering van de platforminstelling te starten.

Lokale vastlegging configureren

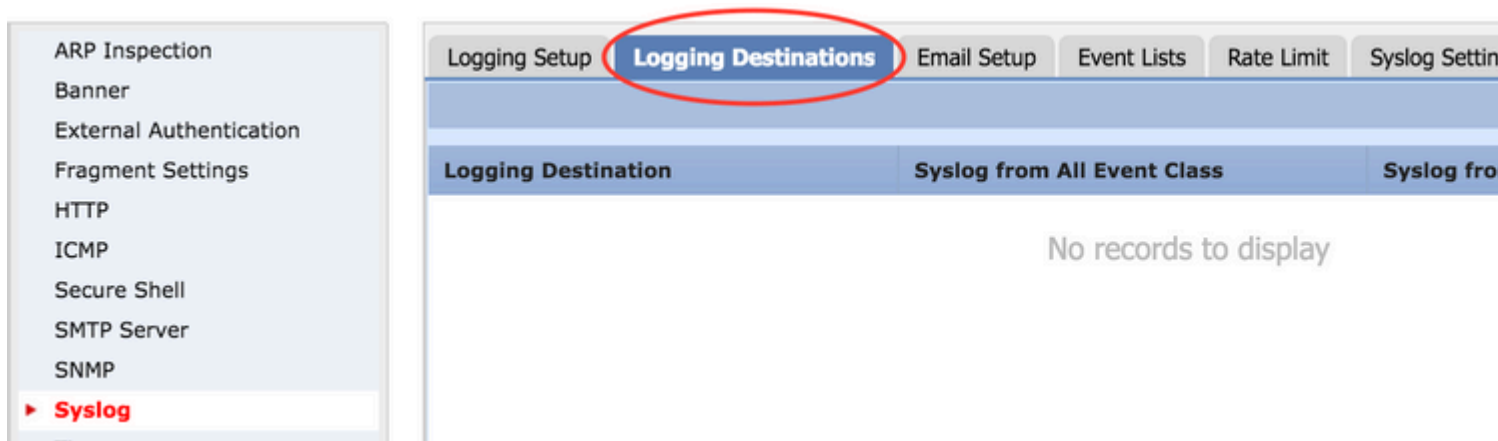
De sectie Bestemming vastlegging kan worden gebruikt om vastlegging te configureren naar specifieke bestemmingen.

De beschikbare interne logboekbestemmingen zijn:

- **Interne buffer:** logbestanden naar de interne logboekbuffer (logboekregistratie gebufferd)
- **Console:** Verstuurt logbestanden naar de console (logboekconsole)
- **SSH-sessies:** logt Syslog in op SSH-sessies (terminal monitor)

Er zijn drie stappen om Lokale vastlegging te configureren.

Stap 1. Kiezen Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations.



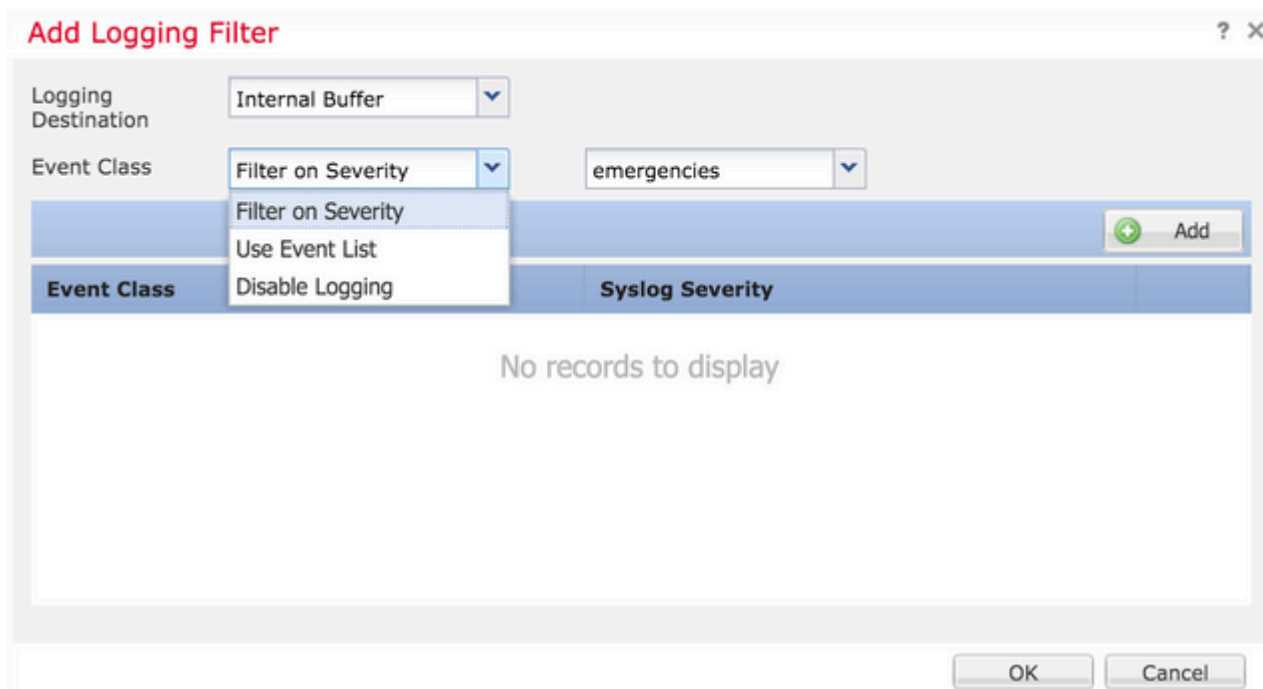
Stap 2. Klik op de knop **Add** om een vastlegging filter toe te voegen voor een specifieke **logging destination**.

Bestemming logboekregistratie: Kies de gewenste bestemming voor de logboekregistratie uit de **Logging Destination** vervolgkeuzelijst als interne buffer, console of SSH-sessies.

Event Class: van de **Event Class** Kies een Event-klasse. Zoals eerder beschreven, zijn Event Classes een set Syslogs die dezelfde functies vertegenwoordigen. Gebeurtenisklassen kunnen op deze manieren worden geselecteerd:

- Filter on Severity: Gebeurtenisklassen filter op basis van de ernst van de Syslogs.
- User Event List: Beheerders kunnen specifieke Event Lists (eerder beschreven) maken met hun eigen aangepaste gebeurtenisklassen en deze in deze sectie doorverwijzen.
- Disable Logging: Gebruik deze optie om logboekregistratie uit te schakelen voor het gekozen doel- en registratieniveau.

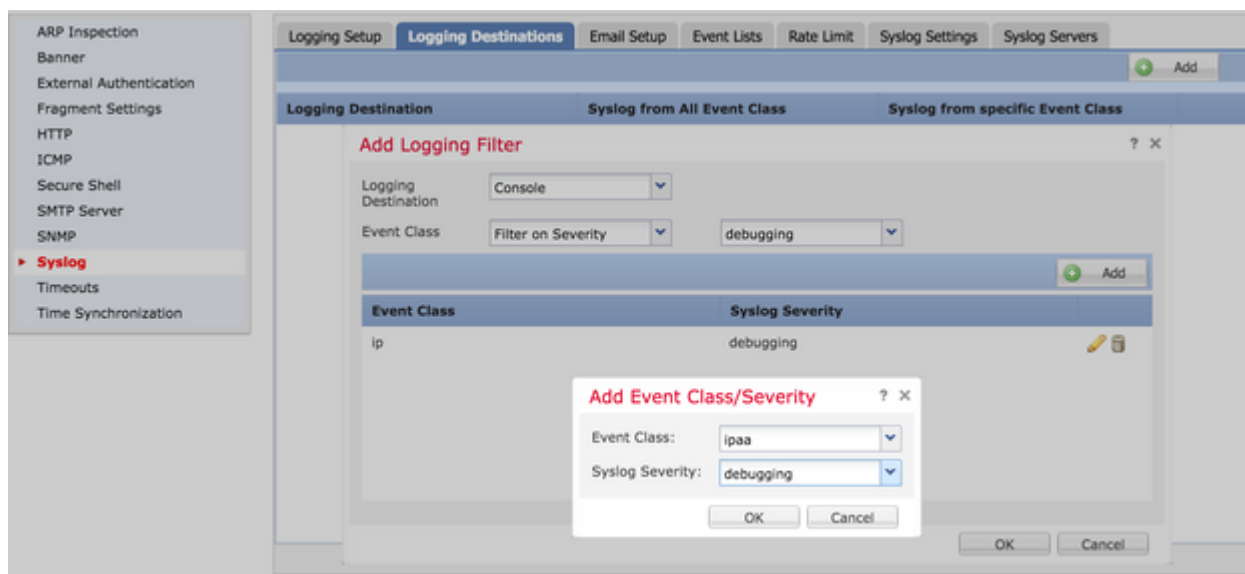
Logniveau: kies het logniveau in de vervolgkeuzelijst. Het bereik van het registratieniveau is van 0 (Noodsituaties) tot 7 (debugging).



Stap 3. Als u een afzonderlijke klasse Event aan dit filter voor vastlegging wilt toevoegen, klikt u op **Add**.

Event Class: Kies de klasse Event uit de Event Class (Functie).

Syslog Severity: Kies de Syslog-ernst uit de Syslog Severity (Functie).



Klik op de knop **OK** zodra het filter is ingesteld om het filter toe te voegen voor een specifieke logbestemming.

Klik op de knop **save** om de platforminstelling op te slaan. Kies **Deploy** Kies het FTD-apparaat op de plaats waar u de wijzigingen wilt toepassen en klik op **Deploy** om de invoering van het platform te starten.

Het externe vastlegging configureren

Als u externe logboekregistratie wilt configureren, kiest u **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations**.

FTD ondersteunt deze soorten externe vastlegging.

- Syslog Server: stuurt logbestanden naar de externe Syslog-server.
- SNMP-trap: Verzendt de logbestanden als SNMP-trap.
- E-mail: Verstuurt de logbestanden via e-mail met een vooraf ingestelde mailrelay server.

De configuratie voor de externe vastlegging en de interne vastlegging zijn hetzelfde. De selectie van Logging bestemmingen bepaalt het type logboekregistratie dat wordt geïmplementeerd. Het is mogelijk om Event Classes te configureren op basis van Custom Event lijsten naar de externe server.

Remote System-server

Syslog servers kunnen worden geconfigureerd om logbestanden op afstand te analyseren en op te slaan vanuit de FTD.

Er zijn drie stappen om externe Syslog-servers te configureren.

Stap 1. Kies **Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Servers**.

Stap 2. Configureer de parameter die aan de Syslog-server gerelateerd is.

- Toestaan dat gebruikersverkeer wordt doorgegeven wanneer TCP-syslog server is uitgeschakeld: Als een TCP-syslog server is geïmplementeerd in het netwerk en niet bereikbaar is, wordt het

netwerkverkeer via de ASA geweigerd. Dit is alleen van toepassing als het transportprotocol tussen de ASA en de Syslog-server TCP is. Controleer de **Allow user traffic to pass when TCP syslog server is down** Schakel dit selectievakje in om verkeer door de interface te laten gaan wanneer de Syslog-server niet actief is.

- **Grootte berichtwachtrij:** De grootte van de berichtwachtrij is het aantal berichten dat in de FTD-wachtrij staat wanneer de externe Syslog-server bezet is en geen logberichten accepteert. De standaardinstelling is 512 berichten en het minimum is 1 bericht. Als 0 in deze optie is opgegeven, wordt de grootte van de wachtrij als onbeperkt beschouwd.

Interface	IP Address	Protocol	Port	EMBLEM
No records to display				

Stap 3. Als u externe systeemserver wilt toevoegen, klikt u op **Add**.

IP Address: van de **IP Address** kies een netwerkobject waarop de Syslog-servers worden vermeld. Als u geen netwerkobject hebt gemaakt, klikt u op het plus-pictogram (+) om een nieuw object te maken.

Protocol: Klik op het **TCP** of **UDP** radioknop voor Syslog-communicatie.

Port: Voer het poortnummer van de Syslog-server in. Standaard is het 514.

Log Messages in Cisco EMBLEM format(UDP only): Klik op de **Log Messages in Cisco EMBLEM format (UDP only)** Schakel dit selectievakje in om deze optie in te schakelen als u berichten in het Cisco EMBLEM-formaat wilt vastleggen. Dit is alleen van toepassing op UDP-gebaseerde syslog.

Available Zones: Voer de veiligheidszones in waarover de Syslog-server bereikbaar is en verplaats deze naar de kolom Geselecteerde zones/interfaces.

Add Syslog Server ? x

IP Address*

Protocol TCP UDP

Port (514 or 1025-65535)

Log Messages in Cisco EMBLEM format(UDP only)

Available Zones

Selected Zones/Interfaces

Klik op de knop **OK** en **save** om de configuratie op te slaan.

Klik op de knop **save** om de platforminstelling op te slaan. Kies **Deploy** Kies het FTD-apparaat op de plaats waar u de wijzigingen wilt toepassen en klik op **Deploy** om de invoering van de platforminstelling te starten.

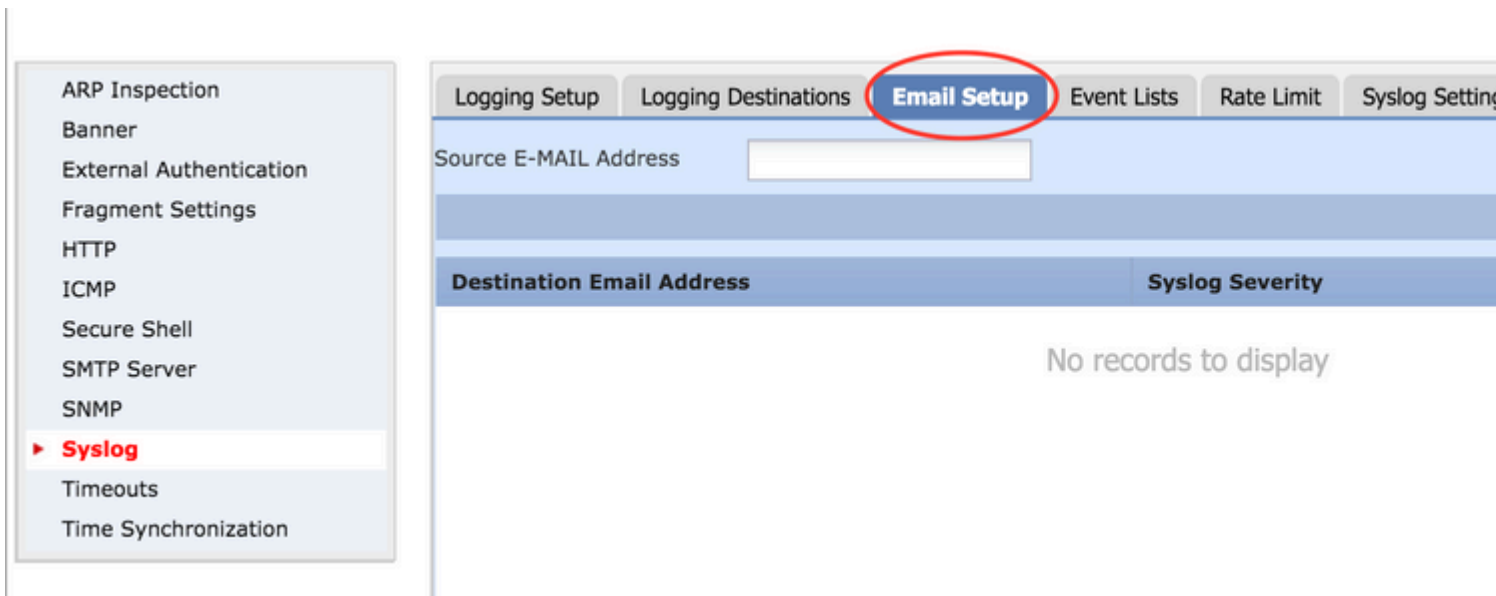
E-mail instellen voor vastlegging

Met FTD kunt u de Syslog naar een specifiek e-mailadres sturen. E-mail kan alleen als een logboekbestemming worden gebruikt als er al een e-mailrelayserver is geconfigureerd.

Er zijn twee stappen om e-mail instellingen te configureren voor de Syslogs.

Stap 1. Kiezen **Device > Platform Setting > Threat Defense Policy > Syslog > Email Setup**.

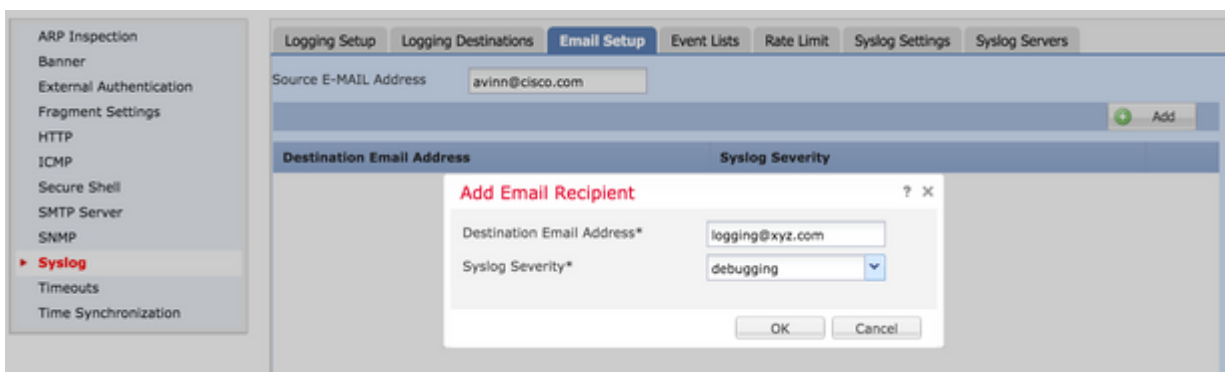
Source E-MAIL Address: Voer het e-mailadres in dat wordt vermeld op alle e-mails die vanuit het FTD worden verstuurd en die de Syslogs bevatten.



Stap 2. Om het doele-mailadres en de ernst van Syslog te configureren klikt u op **Add**.

Destination Email Address: Voer het e-mailadres in van de bestemming waar de Syslog-berichten worden verzonden.

Syslog Severity: Kies de Syslog-ernst uit de Syslog Severity (Functie).



Klik op de knop **OK** om de configuratie op te slaan.

Klik op de knop **Save** om de platforminstelling op te slaan. Kies het FTD-apparaat op de plaats waar u de wijzigingen wilt toepassen en klik op **Deploy** om de invoering van de platforminstelling te starten.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

- Controleer de FTD Syslog-configuratie in de FTD CLI. Log in op de beheerinterface van het FTD en voer de **system support diagnostic-cli** bevel om in de diagnostische CLI te consoleren.

```
> 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
```

- Zorg ervoor dat de Syslog-server bereikbaar is via de FTD. Log in op de FTD-beheerinterface via SSH en controleer de connectiviteit met de ping uit.

```
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
```

- U kunt een pakketopname nemen om de connectiviteit tussen de FTD en de Syslog-server te verifiëren. Log in op de FTD-beheerinterface via SSH en voer de opdracht in `system support diagnostic-cli`. Raadpleeg voor de opdrachten voor pakketopname [ASA Packet Captures met CLI en ASDM Configuration Voorbeeld](#).
- Ervoor zorgen dat het beleid met succes wordt toegepast.

Gerelateerde informatie

- [Cisco Firepower Threat Defence Quick Start Guide voor de ASA](#)
- [Technische ondersteuning en documentatie](#) © Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.