

SNMP-versnellingen voor ASA en FTD configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[ASA-configuratie](#)

[FTD-configuratie beheerde door FDM](#)

[FTD Configuratie beheerd door FMC](#)

[Verifiëren](#)

[Statistieken voor SNMP-servers weergeven](#)

[Vastlegging tonen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u de vellen Simple Network Management Protocol (SNMP) kunt configureren om Syrische berichten te verzenden op Cisco adaptieve security applicatie (ASA) en Firepower Threat Defense (FTD).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van Cisco ASA
- Basiskennis van Cisco FTD
- Basiskennis van het SNMP-protocol

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversie:

- Cisco Firepower Threat Defense voor AWS 6.6.0
- Firepower Management Center versie 6.6.0
- Software voor Cisco adaptieve security applicatie, versie 9.12(3)9

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Cisco ASA en FTD hebben meerdere mogelijkheden om loginformatie te verstrekken. Er zijn echter specifieke locaties waar een snelservice geen optie is. SNMP-traps bieden een alternatief als er een SNMP-server beschikbaar is.

Dit is een handig gereedschap om specifieke berichten te verzenden voor problemen oplossen of bewakingsdoeleinden. Als er bijvoorbeeld een relevant probleem is dat moet worden opgespoord tijdens overvalscenario's, kunnen SNMP-traps voor klasse op zowel FTD als ASA worden gebruikt om zich op die berichten te concentreren.

Nadere informatie over de Syslogklassen is te vinden in [dit document](#).

Dit artikel heeft tot doel configuratievoorbeelden te geven voor ASA met behulp van Commandline Interface (CLI), FTD beheerd door FMC en FTD beheerd door Firepower Devices Manager (FDM).

Als Cisco Defense Orchestrator (CDO) wordt gebruikt voor FTD, moet deze configuratie worden toegevoegd aan de FDM-interface.

Voorzichtig: Voor hoge snelheden wordt aangeraden om een snelheidsbeperking voor syslogberichten te configureren om een impact in andere bewerkingen te voorkomen.

Dit is de informatie die voor alle voorbeelden in dit document wordt gebruikt.

SNMP versie: **SNMPv3**

SNMPv3-groep: **groepsnaam**

SNMPv3-gebruiker: **beheerder-gebruiker** met HMAC SHA-algoritme voor verificatie

IP-adres voor SNMP-server: **10.20.15.12**

ASA/FTD Interface voor communicatie met de SNMP Server: **Buiten de deur**

Bericht-ID Syslog: 111009

Configureren

ASA-configuratie

Deze stappen kunnen worden gebruikt om SNMP Traps op een ASA te configureren volgens de onderstaande informatie.

Stap 1. Configuratie van de berichten die aan de systeemplijst moeten worden toegevoegd.

```
logging list syslog-list message 111009
```

Stap 2. Configuratie van SNMPv3-serverparameters.

```
snmp-server enable
```

```
snmp-server group group-name v3 auth
```

```
snmp-server user admin-user group-name v3 auth sha cisco123
```

Stap 3. Schakel SNMP-trap in.

```
snmp-server enable traps syslog
```

Stap 4. Voeg de SNMP-vallen toe als een houtkapbestemming.

```
logging history syslog-list
```

FTD-configuratie beheerde door FDM

Deze stappen kunnen worden gebruikt om een specifieke systeemlijst te configureren en naar de SNMP-server te verzenden wanneer FTD wordt beheerd door FDM.

Stap 1. Navigeer naar **Exemplaar > Lijstfilters** en selecteer op de **+** knop.

Stap 2. Geef de even lijst een naam en neem de desbetreffende klassen of bericht-ID's op. Selecteer vervolgens OK.

Edit Event List Filter



Name

logging-list

Description

Logs to send through SNMP traps

Severity and Log Class

+

Syslog Range / Message ID

111009

100000 - 999999

[Add Another Syslog Range / Message ID](#)

CANCEL

OK

Stap 3. navigeren naar **Advanced Configuration > FlexConfig > FlexConfig** vanuit het FDM-startscherm en selecteer de **+** knop.

Maak de volgende FlexConfig-objecten met de vermelde informatie:

Naam: **SNMP-server**

Beschrijving (optioneel): **SNMP-serverinformatie**

Modelformulier:

```
snmp-server enable
snmp-server group group-name v3 auth
snmp-server user admin-user group-name v3 auth sha cisco123
snmp-server host outside 10.20.15.12 version 3 admin-user
```

Negatieve sjabloon:

```
no snmp-server host outside 10.20.15.12 version 3 admin-user
no snmp-server user admin-user group-name v3 auth sha cisco123
no snmp-server group group-name v3 auth
no snmp-server enable
```

Edit FlexConfig Object



Name

SNMP-Server

Description

SNMP Server Information

Variables

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template

Expand | Reset

```
1 snmp-server enable
2 snmp-server group group-name v3 auth
3 snmp-server user admin-user group-name v3 auth sha cisco123
4 snmp-server host outside 10.20.15.12 version 3 admin-user
```

Negate Template

Expand | Reset

```
1 no snmp-server host outside 10.20.15.12 version 3 admin-user
2 no snmp-server user admin-user group-name v3 auth sha cisco123
3 no snmp-server group group-name v3 auth
4 no snmp-server enable
```

CANCEL

OK

Naam: **SNMP-Traps**

Beschrijving (optioneel): **SNMP-trap inschakelen**

Modelformulier:

```
snmp-server enable traps syslog
```

Negatieve sjabloon:

```
no snmp-server enable traps syslog
```

Edit FlexConfig Object



Name

SNMP-Traps

Description

Enable SNMP traps

Variables

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template

Expand | Reset

```
1 snmp-server enable traps syslog
```

Negate Template

Expand | Reset

```
1 no snmp-server enable traps syslog
```

CANCEL

OK

Naam: **Vastlegging**

Description (optioneel): **object om SNMP-overtrekposten in te stellen**

Modelformulier:

```
logging history logging-list
```

Negatieve sjabloon:

```
no logging history logging-list
```

Create FlexConfig Object



Name

Logging-List

Description

Syslog list to send through SNMP traps



Variables

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template

Expand | Reset

```
1 logging list syslog-list message 111009
2 logging trap syslog-list
```

Negate Template

Expand | Reset

```
1 no logging trap syslog-list
2 no logging list syslog-list message 111009
```

CANCEL

OK

Stap 4. Navigeer naar **geavanceerde configuratie > FlexConfig > FlexConfig** en voeg alle in de vorige stap gemaakte objecten toe. De volgorde is irrelevant aangezien de afhankelijke opdrachten in hetzelfde object (SNMP-server) zijn opgenomen. Selecteer **Opslaan** als de drie objecten aanwezig zijn en het gedeelte **Voorbeeld** geeft de lijst met opdrachten weer.

Successfully saved.

Group List

+

1. Logging-history

2. SNMP-Server

3. SNMP-Traps

Preview

Expand

```
1 logging history logging-list
2 snmp-server enable
3 snmp-server group group-name v3 auth
4 snmp-server user admin-user group-name v3 auth sha cisco123
5 snmp-server host outside 10.20.15.12 version 3 admin-user
6 snmp-server enable traps syslog
```

SAVE

Stap 5. Selecteer het pictogram **Deployment** om wijzigingen toe te passen.

FTD Configuratie beheerd door FMC

De voorbeelden hierboven illustreren soortgelijke scenario's als de voorgaande, maar deze wijzigingen worden op het VCC uitgevoerd en vervolgens in een door het VCC beheerde VHV's aangebracht. SNMPv2 kan ook worden gebruikt. [In dit artikel](#) wordt uitgelegd hoe u een SNMP-server met deze versie op FTD kunt opzetten met behulp van FMC-beheer.

Stap 1. Navigeer naar **Apparaten > Instellingen platform** en selecteer **Bewerken** op het aan het beheerde apparaat toegewezen beleid om de configuratie op toe te passen.

Stap 2. Navigeer naar **SNMP** en controleer de optie **SNMP servers inschakelen**.

Overview Analysis Policies **Devices** Objects AMP Intelligence ✔ Deploy System Help ▾

Device Management NAT VPN ▾ QoS **Platform Settings** FlexConfig Certificates

FTD-PS You have unsaved changes Save

Enter Description Policy A

- ARP Inspection
- Banner
- DNS
- External Authentication
- Fragment Settings
- HTTP
- ICMP
- Secure Shell
- SMTP Server
- SNMP**
- SSL
- Syslog
- Timeouts
- Time Synchronization
- Time Zone
- UCAPL/CC Compliance

Enable SNMP Servers

Read Community String

Confirm

System Administrator Name

Location

Listen Port (1 - 65535)

Hosts Users SNMP Traps

➕ Add

Interface	Network	SNMP Version	Poll/Trap	Trap Port	Username
No records to display					

Stap 3. Selecteer het tabblad **Gebruikers** en selecteer de knop **Add**. Vul de gebruikersinformatie in.

Add Username ? X

Security Level	Auth
Username*	user-admin
Encryption Password Type	Clear Text
Auth Algorithm Type	SHA
Authentication Password*	••••••••
Confirm*	••••••••
Encryption Type	
Encryption Password	
Confirm	

OK Cancel

Stap 4. Selecteer **Add** in het tabblad **Hosts**. Vul de informatie in met betrekking tot de SNMP-server. Als u een interface in plaats van een zone gebruikt, zorg er dan voor dat u de interfacenaam handmatig in het rechterhoekgedeelte kunt toevoegen. Selecteer OK als alle benodigde informatie is opgenomen.

Add SNMP Management Hosts

IP Address*

SNMP Version

Username

Community String

Confirm

Poll

Trap

Trap Port (1 - 65535)

Reachable By:

Device Management Interface *(Applicable from v6.6.0 and above)*

Security Zones or Named Interface

Available Zones

Selected Zones/Interfaces

outside

Stap 5. Selecteer het tabblad **SNMP-trappen** en controleer het vakje **Snel**. Zorg ervoor dat u alle andere vinkjes verwijdert als deze niet nodig zijn.

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

FTD-PS You have unsaved changes Save

Enter Description Policy A

- ARP Inspection
- Banner
- DNS
- External Authentication
- Fragment Settings
- HTTP
- ICMP
- Secure Shell
- SMTP Server
- SNMP**
- SSL
- Syslog
- Timeouts
- Time Synchronization
- Time Zone
- UCAPL/CC Compliance

Enable SNMP Servers

Read Community String

Confirm

System Administrator Name

Location

Listen Port (1 - 65535)

Hosts Users **SNMP Traps**

Enable Traps All SNMP Syslog

Standard

Authentication

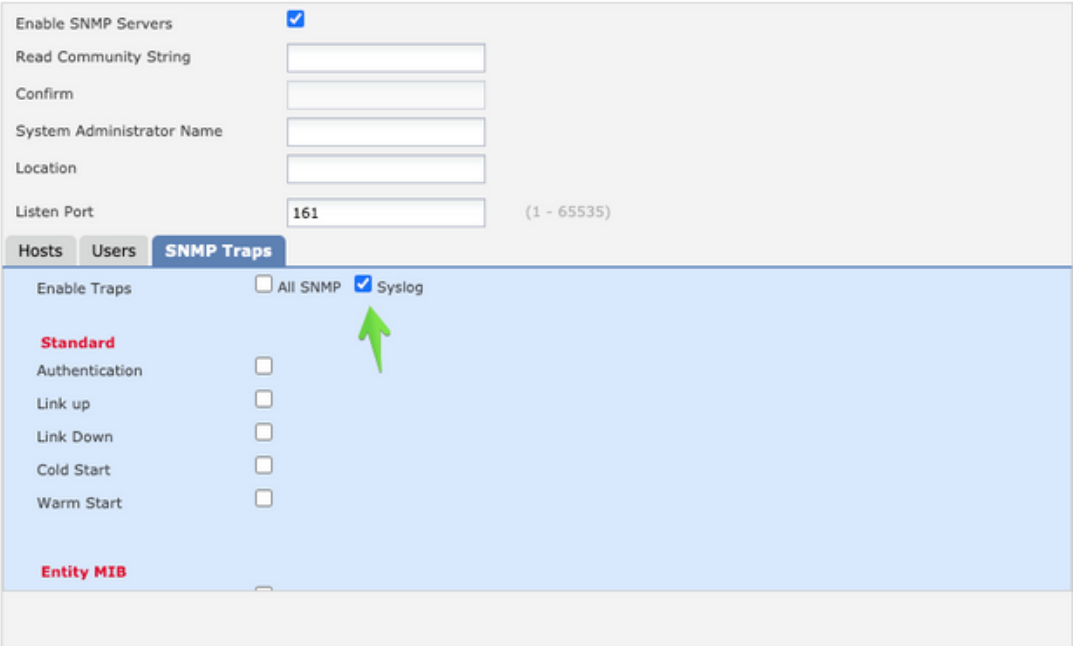
Link up

Link Down

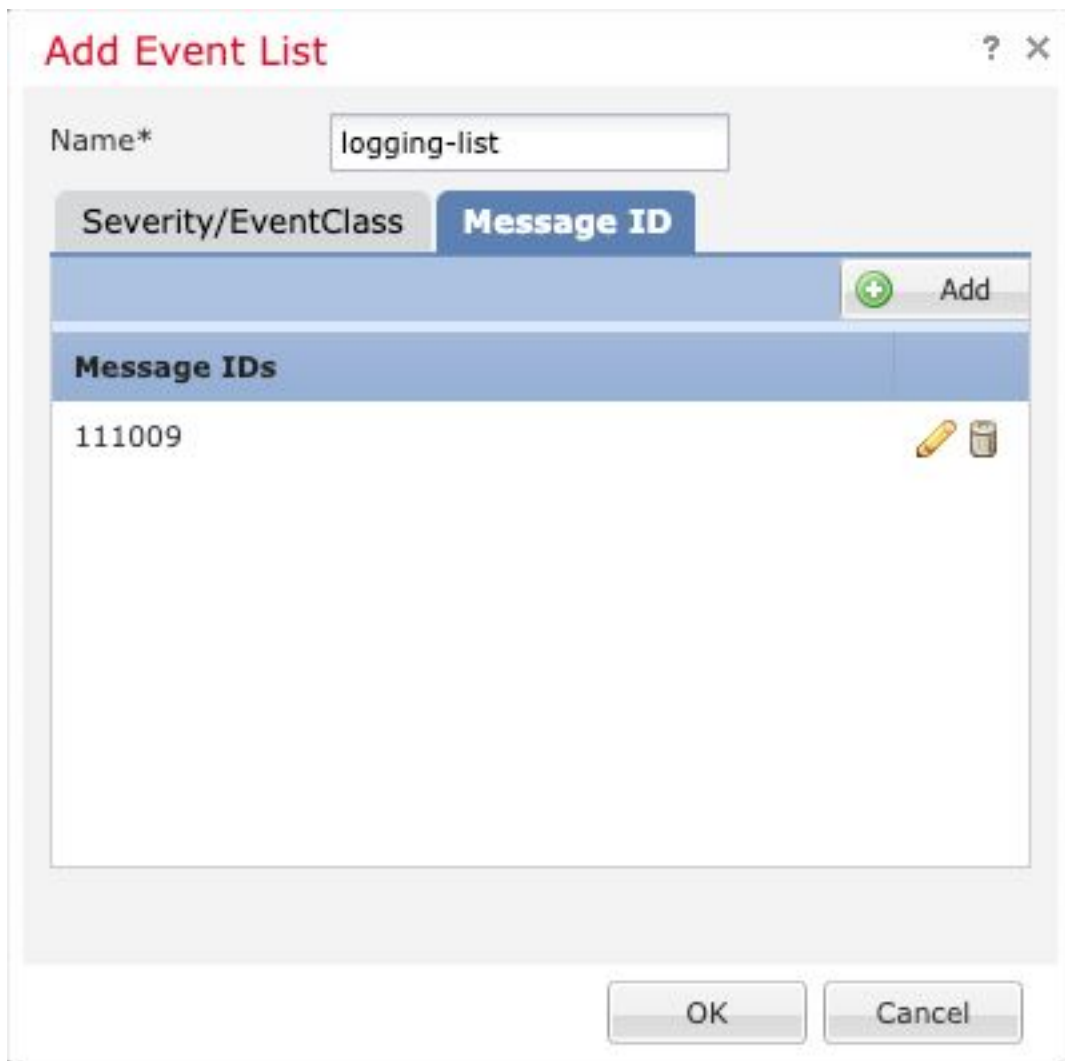
Cold Start

Warm Start

Entity MIB



Stap 6. Navigeer naar **Syslog** en selecteer het tabblad **Event Lists**. Selecteer de knop **Toevoegen**. Voeg een naam en de berichten toe die in de lijst moeten worden opgenomen. Selecteer **OK** om verder te gaan.

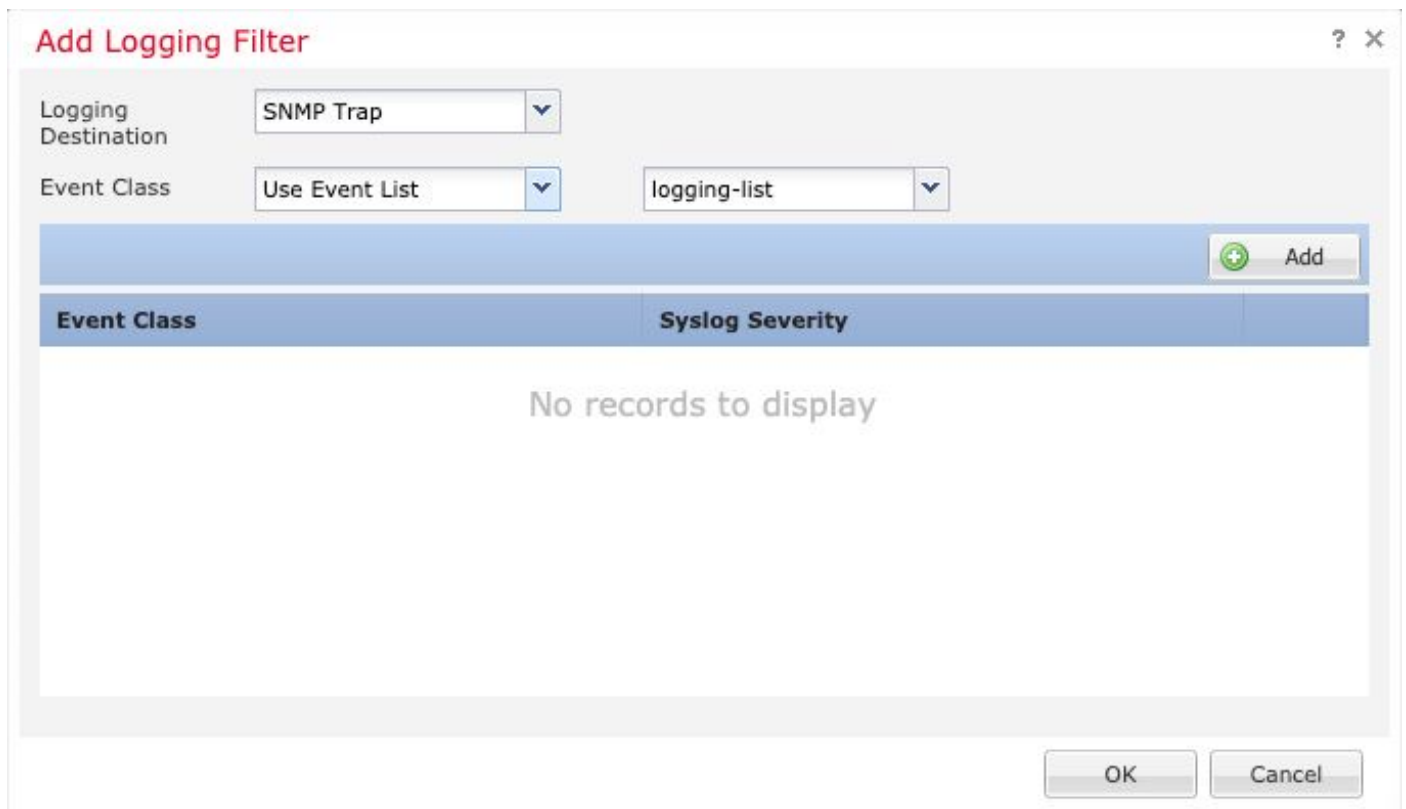


Stap 7. Selecteer het tabblad **Vastlegging** en selecteer de knop **Toevoegen**.

Verander de Logging Destination in **SNMP Trap**.

Selecteer **Gebruikerslijst** en kies de lijst met gebeurtenissen die in Stap 6 naast deze lijst is gemaakt.

Selecteer **OK** om deze sectie te bewerken.



Stap 8. Selecteer de knop **Opslaan** en voer de wijzigingen in het beheerde apparaat in.

Verifiëren

De onderstaande opdrachten kunnen zowel in FTD CLISH als in ASA CLI worden gebruikt.

Statistieken voor SNMP-servers weergeven

De opdracht "**show snmp-server statistics**" geeft informatie over hoe vaak een val is verstuurd. Deze teller kan andere vallen bevatten.

```
# show snmp-server statistics
0 SNMP packets input
0 Bad SNMP version errors
0 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors
0 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
0 Get-next PDUs
0 Get-bulk PDUs
0 Set-request PDUs (Not supported)
2 SNMP packets output
0 Too big errors (Maximum packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors
0 Response PDUs
2 Trap PDUs
```

De bericht-ID die in dit voorbeeld wordt gebruikt, wordt geactiveerd zodra een gebruiker een opdracht uitvoert. Telkens wanneer een opdracht "show" wordt gegeven, neemt de teller toe.

Vastlegging tonen

De "**show logging setting**" geeft informatie over de berichten die door elke bestemming worden verstuurd. History logging geeft de tellers voor SNMP vallen aan. De loggegevens van de Trap zijn verwant aan Syslog gastheren tellers.

```
# show logging setting
Syslog logging: enabled
Facility: 20
Timestamp logging: enabled
Hide Username logging: enabled
Standby logging: disabled
Debug-trace logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level debugging, 30 messages logged
Trap logging: level debugging, facility 20, 30 messages logged
Global TCP syslog stats:
NOT_PUTABLE: 0, ALL_CHANNEL_DOWN: 0
CHANNEL_FLAP_CNT: 0, SYSLOG_PKT_LOSS: 0
PARTIAL_REWRITE_CNT: 0
Permit-hostdown logging: disabled
History logging: list syslog-list, 14 messages logged
Device ID: disabled
Mail logging: disabled
ASDM logging: disabled
```

Geef de opdracht "**show logging wachtrij**" uit om er zeker van te zijn dat er geen berichten achterblijven.

```
# show logging queue

Logging Queue length limit : 512 msg(s)
0 msg(s) discarded due to queue overflow
0 msg(s) discarded due to memory allocation failure
Current 0 msg on queue, 231 msgs most on queue
```

Gerelateerde informatie

- [Cisco ASA Series NextGeneration Systems](#)
- [CLI-boek 1: Cisco ASA Series Next-Generation Operations CLI Configuration Guide, 9.12](#)
- [SNMP configureren op FirePOWER NGFW-applicaties](#)