Syslog configureren op FirePOWER FXOS-applicaties

Inhoud

Inleiding

Dit document beschrijft hoe u het systeem voor configuratie, verificatie en probleemoplossing kunt configureren op FirePOWER Xtensible Operating System (FXOS) apparatuur.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- 1x FPR4120 met FXOS-softwareversie 2.2(1.70)
- 1x FPR210 met ASA-softwareversie 9.9(2)
- 1x FPR2110 met FTD-softwareversie 6.2.3
- 1x SLB-server

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

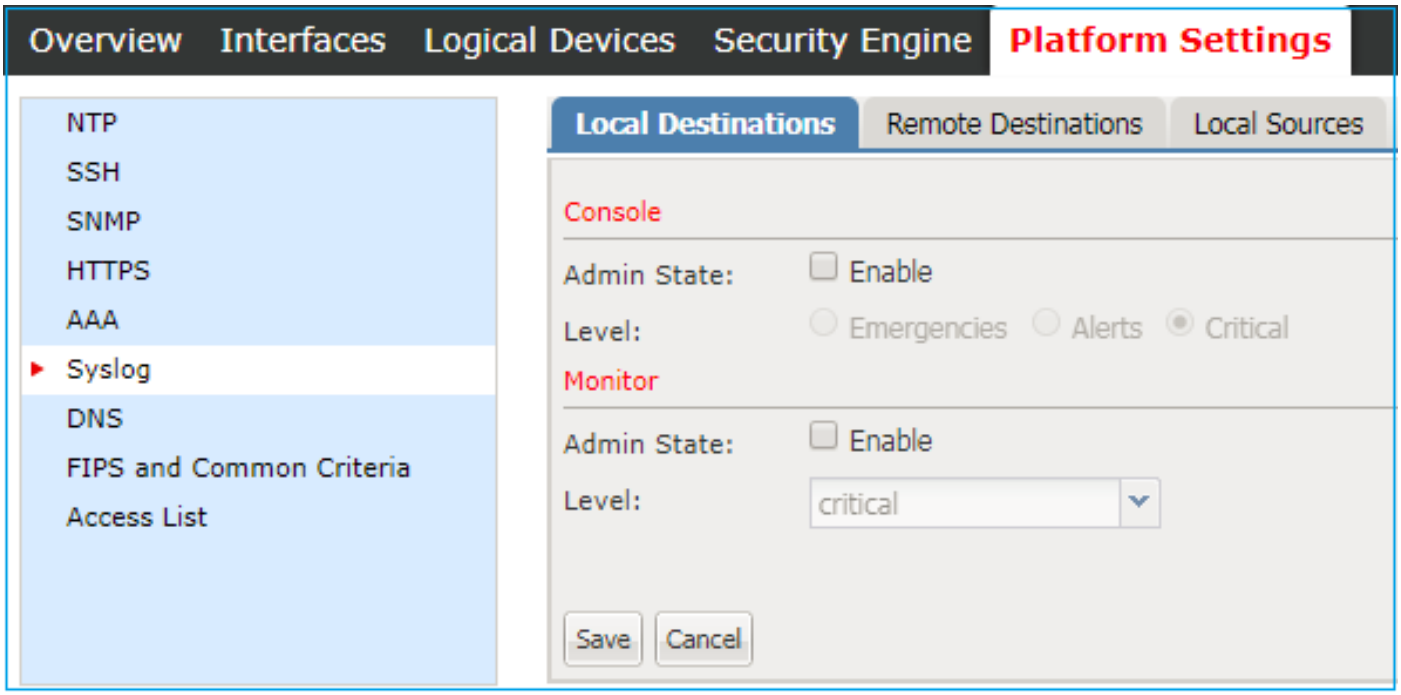
opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

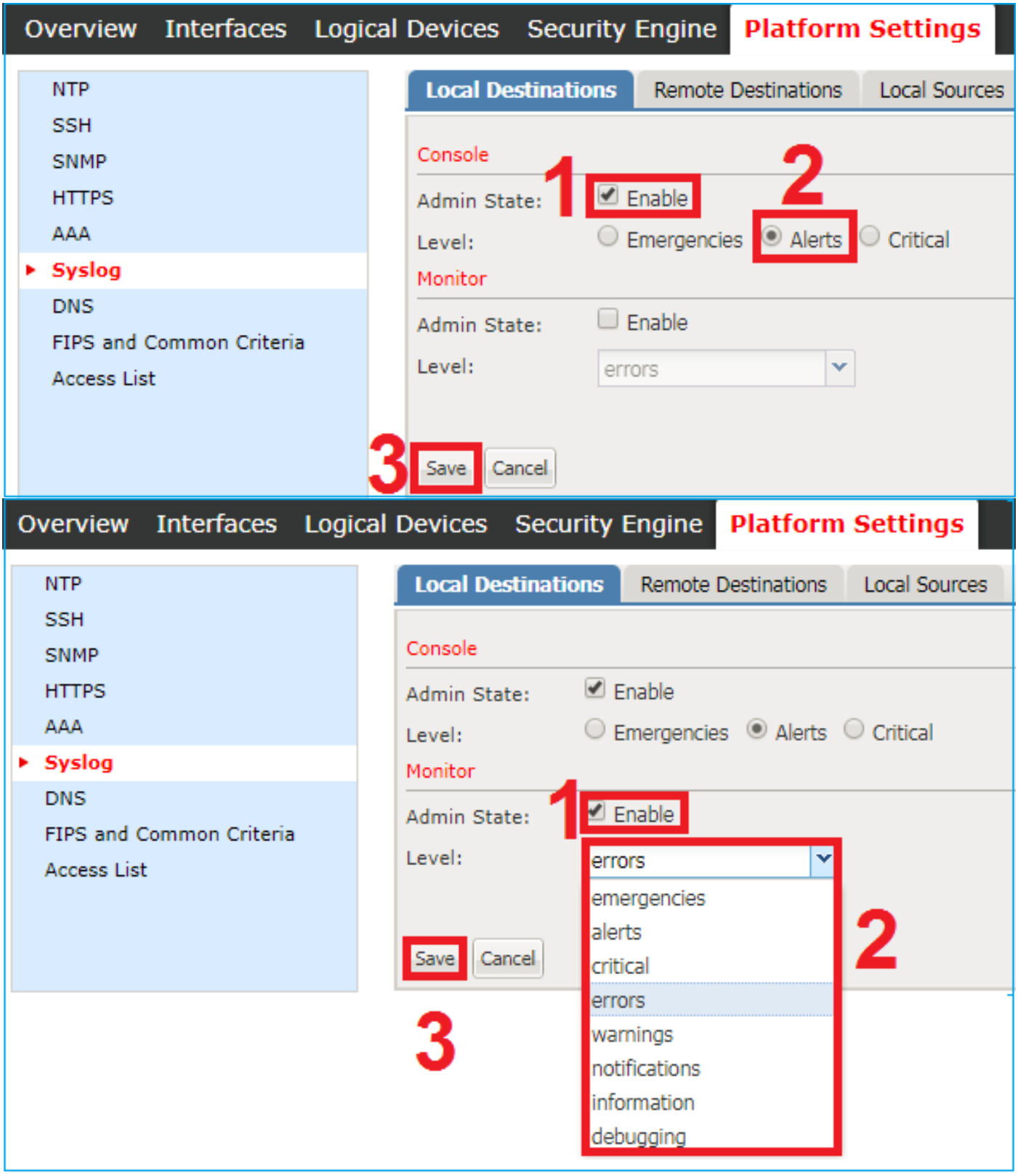
Configuratie van symbolen met FXOS-gebruikersinterface (FPR4100/FPR9300)

FXOS heeft een eigen verzameling systeemmeldingen die mogelijk worden ingeschakeld en ingesteld vanuit Firepower Chassis Manager (FCM).

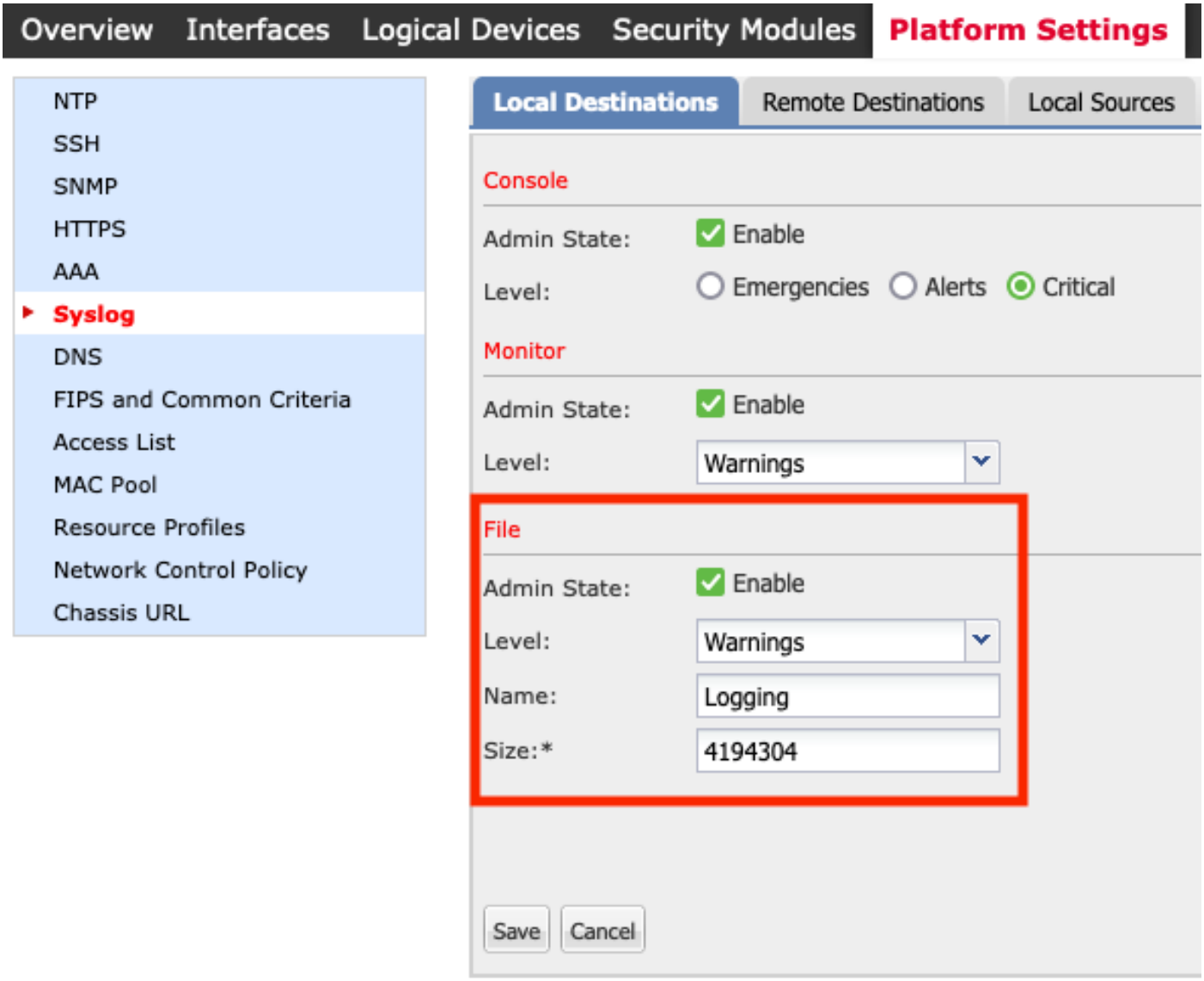
Stap 1. Navigeer naar **platform instellingen > SLUG.**



Stap 2. Onder **Lokale bestemmingen** kunt u SLOGberichten op console inschakelen voor niveaus 0-2 of lokale controle van SLOG voor elk niveau dat lokaal is opgeslagen. Controleer of alle geselecteerde ernst niveaus ook voor beide methoden worden weergegeven: console en monitor.



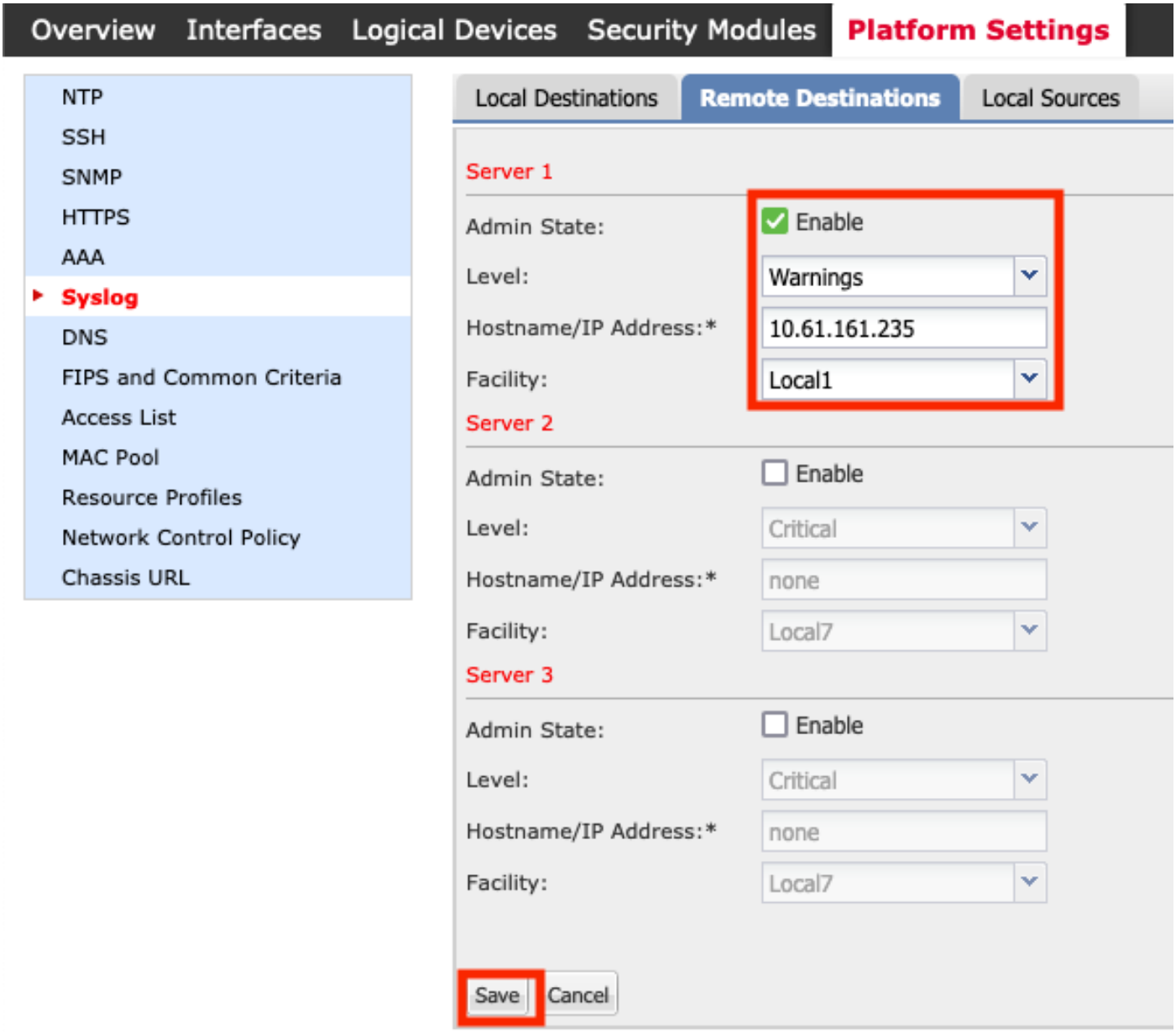
Vanaf FXOS versie 2.3.1 kunt u ook via GUI een lokale bestandstoetsing voor Syslog-berichten configureren:



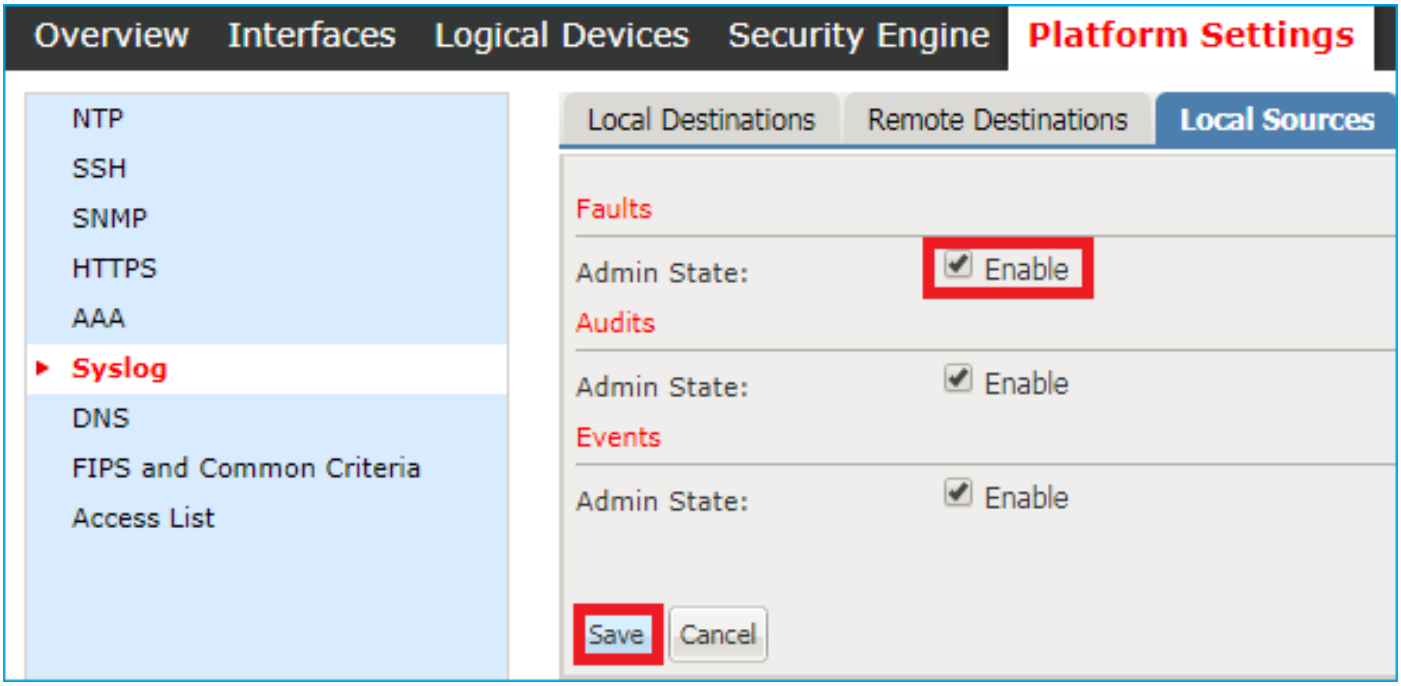
Opmerking: De bestandsgrootte kan alleen een grootte van 4096 tot 4194304 bytes hebben.

Opmerking: In de versie pre-2.3.1 FXOS is de bestandsconfiguratie alleen beschikbaar via CLI.

U kunt ook maximaal 3 Remote SLUG-servers configureren vanaf het tabblad **Afstandsbestemmingen**. Elke server kan worden gedefinieerd als een bestemming voor verschillende boodschappen met de ernst van het systeemvak en wordt gemarkeerd met een andere lokale voorziening.



Stap 3. Ten slotte selecteert u extra **lokale bronnen** voor de systeemmeldingen. FXOS kan worden gebruikt als standaardbronfouten, auditberichten en/of gebeurtenissen.



Configureren vanuit FXOS CLI (FPR4100/FPR9300)

Het equivalent van sectie **Lokale bestemmingen** configureren via CLI:

```
FP4120-A /monitoring # enable syslog console
FP4120-A /monitoring* # set syslog console level critical
FP4120-A /monitoring* # enable syslog monitor
FP4120-A /monitoring* # set syslog monitor level warning
FP4120-A /monitoring* # commit-buffer
```

Configureer via CLI de equivalente van sectie **Remote Destinaties**:

```
FP4120-A /monitoring # enable syslog remote-destination server-1
FP4120-A /monitoring* # set syslog remote-destination server-1 facility local1
FP4120-A /monitoring* # set syslog remote-destination server-1 level warning
FP4120-A /monitoring* # set syslog remote-destination server-1 hostname 10.61.161.235
FP4120-A /monitoring* # commit-buffer
```

Configuratie via CLI de equivalent van sectie **Lokale bronnen**:

```
FP4120-A /monitoring # enable syslog source audits
FP4120-A /monitoring* # enable syslog source events
FP4120-A /monitoring* # enable syslog source faults
FP4120-A /monitoring* # commit-buffer
```

Daarnaast kunt u een lokaal bestand als sneleindbestemming inschakelen. Deze meldingen kunnen worden weergegeven met behulp van de opdrachten die **vastlegging** of **logbestand tonen**:

```
FP4120-A /monitoring # enable syslog file
FP4120-A /monitoring* # set syslog file level warning
FP4120-A /monitoring* # set syslog file name Logging
FP4120-A /monitoring* # commit-buffer
```

Opmerking: De standaardgrootte van dit bestand is het maximale aantal (4194304 bytes).

Controleer de configuratie via CLI

De configuratie kan worden geverifieerd en geconfigureerd van de **monitoring** van de reikwijdte:

```
FP4120-A# scope monitoring
FP4120-A /monitoring # show syslog

console
    state: Enabled
    level: Critical

monitor
    state: Enabled
    level: warning

file
    state: Enabled
    level: warning
    name:  Logging
    size:  4194304

remote destinations
    Name     Hostname             State    Level         Facility
    -------- -------------------- -------- ------------ --------
    Server 1 10.61.161.235        Enabled  warning     Local1
    Server 2 none                 Disabled Critical      Local7
    Server 3 none                 Disabled Critical      Local7

sources
    faults: Enabled
    audits: Enabled
    events: Enabled
```

U kunt ook een volledigere uitvoer van FXOS CLI krijgen met de opdracht **show logging**:

```
FP4120-A(fxos)# show logging

Logging console:                enabled (Severity: critical)
Logging monitor:                enabled (Severity: warning)
Logging linecard:               enabled (Severity: notifications)
Logging fex:            enabled (Severity: notifications)
Logging timestamp:              Seconds
Logging server:                 enabled
{10.61.161.235}
        server severity:        warning
        server facility:        local1
        server VRF:             management
Logging logfile:                enabled
        Name - Logging: Severity - warning Size - 4194304

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     3                       7
acllog                  2                       7
```

aclmgr	3	7
afm	3	7
assoc_mgr	7	7
auth	0	7
authpriv	3	7
bcm_usd	3	7
bootvar	5	7
callhome	2	7
capability	2	7
capability	2	7
cdp	2	7
cert_enroll	2	7
cfs	3	7
clis	7	7
confcheck	2	7
copp	2	7
cron	3	7
daemon	3	7
device-alias	3	7
epp	5	7
eth_port_channel	5	7
eth_port_sec	2	7
ethpc	2	7
ethpm	5	7
evmc	5	7
fabric_start_cfg_mgr	2	7
fc2d	2	7
fcdomain	3	7
fcns	2	7
fcpc	2	7
fcs	2	7
fdmi	2	7
feature-mgr	2	7
fex	5	7
flogi	2	7
fspf	3	7
ftp	3	7
fwm	6	7
ifmgr	5	7
igmp_1	5	7
ip	3	7
ipqosmgr	4	7
ipv6	3	7
kern	3	7
l3vm	5	7
lacp	2	7
ldap	2	7
ldap	2	7
licmgr	6	7
lldp	2	7
local0	3	7
local1	3	7
local2	3	7
local3	3	7
local4	3	7
local5	3	7
local6	3	7
local7	3	7
lpr	3	7
m2rib	2	7
mail	3	7
mcm	2	7
monitor	3	7
mrib	5	7

```
msp                     5                       7
mvsh                    2                       7
news                    3                       7
nfp                     2                       7
nohms                   2                       7
nsmgr                   5                       7
ntp                     2                       7
otm                     3                       7
pfstat                  2                       7
pim                     5                       5
platform                5                       7
plugin                  2                       7
port                    5                       7
port-channel            5                       7
port-profile            2                       7
port-resources          5                       7
private-vlan            3                       7
qd                      2                       7
radius                  3                       7
rdl                     2                       7
res_mgr                 5                       7
rib                     2                       7
rlir                    2                       7
rpm                     5                       7
rscn                    2                       7
sal                     2                       7
scsi-target             2                       7
securityd               3                       7
smm                     4                       7
snmpd                   2                       7
span                    3                       7
stp                     3                       7
syslog                  3                       7
sysmgr                  3                       7
tacacs                  3                       7
u6rib                   5                       7
udld                    5                       7
urib                    5                       7
user                    3                       7
uucp                    3                       7
vdc_mgr                 6                       7
vim                     5                       7
vlan_mgr                2                       7
vmm                     5                       7
vms                     5                       7
vntag_mgr               6                       7
vsan                    2                       7
vshd                    5                       7
wwn                     3                       7
xmlma                   3                       7
zone                    2                       7
zschk                   2                       7

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)

2017 Nov 26 16:49:19 FP4120-5-A %$ VDC-1 %$ %LOCAL0-2-SYSTEM_MSG: Test-Syslog - ucssh[18553]
```

Controleer dat er zwarte berichten verschijnen onder de terminalmonitor

Als de sislogmonitor is ingeschakeld, worden de slogberichten onder FXOS CLI geplaatst

wanneer de monitorterminal is ingeschakeld.

```
FP4120-A(fxos)# terminal monitor
2017 Nov 26 16:39:35 FP4120-5-A %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid 1910369168]
[client 127.0.0.1:34975] AH01964: Connection to child 40 established (server 10.62.148.187:443)
- httpd[23982]
2017 Nov 26 16:39:36 FP4120-5-A %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid 1908272016]
[client 127.0.0.1:34977] AH01964: Connection to child 42 established (server 10.62.148.187:443)
- httpd[23982]
2017 Nov 26 16:39:36 FP4120-5-A %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid 1911417744]
(70014)End of file found: [client 127.0.0.1:34972] AH01991: SSL input filter read failed. -
httpd[23982]
```

Controleer de service voor de afstandsbediening ingesteld

Controleer dat er berichten op de Syslog-server worden ontvangen.

Date	Time	Priority	Hostname	Message
11-26-2017	16:03:03	Local1.Info	10.62.148.187	: 2017 Nov 26 15:40:46 UTC: %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid
11-26-2017	16:03:03	Local1.Info	10.62.148.187	: 2017 Nov 26 15:40:46 UTC: %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid
11-26-2017	16:03:01	Local1.Info	10.62.148.187	: 2017 Nov 26 15:40:44 UTC: %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid

Leg verkeer op FXOS CLI vast met het hulpmiddel EtherAnalyzer om te bevestigen dat Syrische berichten door FXOS worden gegenereerd en verzonden.

In dit voorbeeld komt de bestemming van het bericht overeen met de lokale SLOGserver (10.61.161.235), de vlag van de voorziening (Local1) en de ernst van het bericht (6):

```
FP4120-A(fxos)# ethanalyzer local interface mgmt capture-filter "host 10.61.161.235 && udp port
514"
Capturing on eth0
wireshark-broadcom-rcpu-dissector: ethertype=0xde08, devicetype=0x0
2017-11-26 16:01:38.881829 10.62.148.187 -> 10.61.161.235Syslog LOCAL1.INFO: : 2017 Nov 26
16:01:38 UTC: %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid 1799220112] (70014)End of file
found: [client 127.0.0.1:51015] AH01991: SSL input filter read failed. - httpd[23982]
2017-11-26 16:01:38.882574 10.62.148.187 -> 10.61.161.235 Syslog LOCAL1.INFO: : 2017 Nov 26
16:01:38 UTC: Nov 26 16:01:37 %KERN-6-SYSTEM_MSG: [363494.943876] device eth0 entered
promiscuous mode - kernel
2017-11-26 16:01:38.883333 10.62.148.187 -> 10.61.161.235 Syslog LOCAL1.INFO: : 2017 Nov 26
16:01:38 UTC: %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid 1782442896] (70014)End of file
found: [client 127.0.0.1:51018] AH01991: SSL input filter read failed. - httpd[23982]
```

Controleer dat het lokale logbestand correct is geregistreerd vanuit FXOS

```
FP4120-A(fxos)# show logging logfile
2017 Nov 26 15:20:22 FP4120-5-A %SYSLOG-1-SYSTEM_MSG : Logging logfile (messages) cleared by
user
2017 Nov 26 16:24:21 FP4120-5-A %USER-7-SYSTEM_MSG: Semaphore lock success   - aaad
2017 Nov 26 16:24:21 FP4120-5-A %USER-7-SYSTEM_MSG: accounting_sem_unlock Semaphore unlock
succeeded   - aaad
2017 Nov 26 16:24:21 FP4120-5-A %USER-7-SYSTEM_MSG: Semaphore lock success   - aaad
```

Testsyslogberichten genereren

Er is ook de mogelijkheid om Syslog-berichten van elke ernst op verzoek te genereren voor testdoeleinden via CLI. Op deze manier kunt u in zeer actieve Syslog-servers een specifieker filter definiëren om u te helpen bevestigen dat de Syslog-berichten correct worden verstuurd:

```
FP4120-A /monitoring # send-syslog critical Test-Syslog
```

Dit bericht wordt doorgestuurd naar een willekeurige Syslog-bestemming en kan handig zijn in scenario's waar filtering van een specifieke Syslog-bron niet mogelijk is:

```
FP4120-A(fxos)# show logging logfile
2017 Nov 26 16:49:19 FP4120-5-A %$ VDC-1 %$ %LOCAL0-2-SYSTEM_MSG: Test-Syslog - ucssh[18553]
```

Date	Time	Priority	Hostname	Message
11-26-2017	17:11:36	Local1.Critical	10.62.148.187	: 2017 Nov 26 16:49:19 UTC: %LOCAL0-2-SYSTEM_MSG: Testing-Syslog - ucssh[18553]

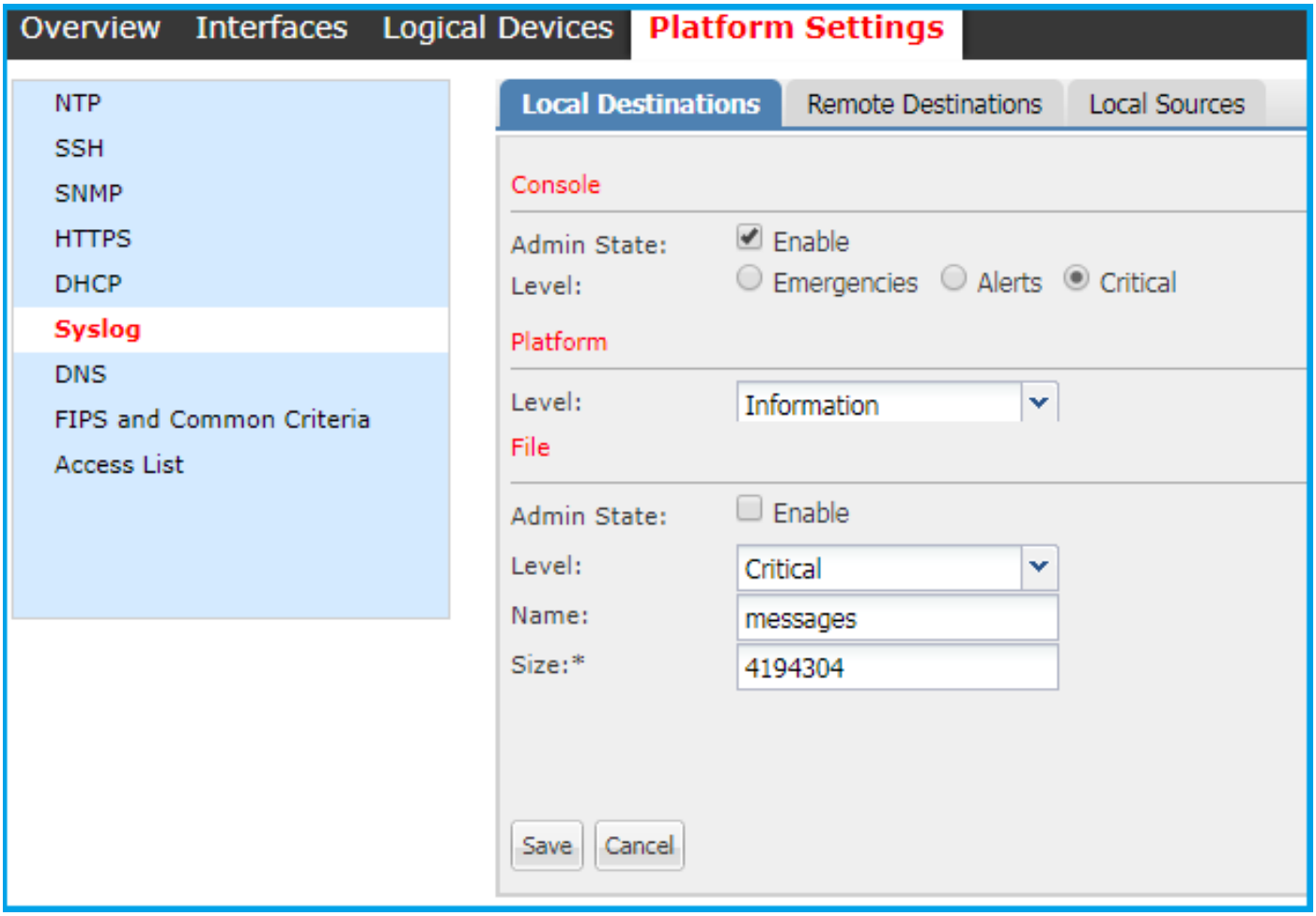
FXOS-systeem in FirePOWER 2100 applicaties

ASA logische apparaat in FPR2100

Er zijn twee belangrijke verschillen tussen de configuratie van Syslog voor Firepower 4100/9300 en Firepower 2100 apparaten met ASA-software.

1. In Firepower 2100 wordt de platform logging mogelijk door de standaardinstelling en kan niet worden uitgeschakeld.

2. Er is geen monitorhoutkap door het feit dat de monitorterminal niet bestaat in FP2100-platforms.



Zowel **Remote Destinaties** als **Local Resources** secties zijn identiek aan de andere platforms.

De logbestanden en de actieve logbestanden van het platform zijn niet toegankelijk via CLI-opdrachten.

FTD logisch apparaat in FPR2100

In FPR2100, waar een FTD-apparaat is geïnstalleerd, zijn er twee belangrijke verschillen ten opzichte van de andere topologieën:

1. Het bron IP-adres is hetzelfde als het logische apparaat Syslog-berichten.

2. Alle FXOS-berichten worden gebruikt voor SLOG-ID, het bericht voor generieke processen van ASA 1990-199019

```
firepower# show logging | include 1990
%ASA-6-199018: May 11 18:10:55 fp2100a port-manager: Informational: Ethernet1/12: admin state changed to down
%ASA-7-199019: May 11 18:10:55 fp2100a port-manager: LINK STATE CHANGE: port 50, new state 0/0/0
%ASA-2-199014: May 11 18:10:56 fp2100a port-manager: Alert: Ethernet1/12 link changed to DOWN
%ASA-6-199018: May 11 18:10:56 fp2100a port-manager: Informational: Ethernet1/12 speed changed to Unknown
```

In dit voorbeeld zijn er de interface shutdown Syslog berichten.

FAQ

Welke is de standaardpoort die door Syslog gebruikt wordt?

Standaard gebruikt Syslog UDP-poort 514

Kun je Syslog configureren via TCP?

Syslowakije via TCP wordt alleen ondersteund voor FPR2100 met FTD-apparaten waar FXOS-systemen worden geïntegreerd in de ASA-berichten

Gerelateerde informatie

- FXOS CLI-configuratiegids
- Technische ondersteuning en documentatie – Cisco Systems