Firepower FXOS 어플라이언스에 Syslog 구성

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[구성](#)
[FXOS 사용자 인터페이스에서 Syslog 구성(FPR4100/FPR9300)](#)
[FXOS CLI에서 Syslog 구성(FPR4100/FPR9300)](#)
[CLI를 통해 컨피그레이션 확인](#)
[Syslog 메시지가 터미널 모니터 아래에 나타나는지 확인합니다.](#)
[구성된 원격 호스트에 대한 서비스 확인](#)
[FXOS에서 로컬 로그 파일이 올바르게 로깅되는지 확인합니다.](#)
[테스트 Syslog 메시지 생성](#)
[Firepower 2100 어플라이언스의 FXOS Syslog](#)
[FPR2100의 ASA 논리적 디바이스](#)
[FPR2100의 FTD 논리적 디바이스](#)
[FAQ](#)
[관련 정보](#)

소개

이 문서에서는 FXOS(Firepower eXtensible Operating System) 어플라이언스에서 Syslog를 구성, 확인 및 트러블슈팅하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- FXOS 소프트웨어 버전 2.2(1.70)가 포함된 1x FPR4120
- 1x FPR2110, ASA 소프트웨어 버전 9.9(2)
- 1x FPR2110(FTD 소프트웨어 버전 6.2.3 포함)
- Syslog 서버 1개

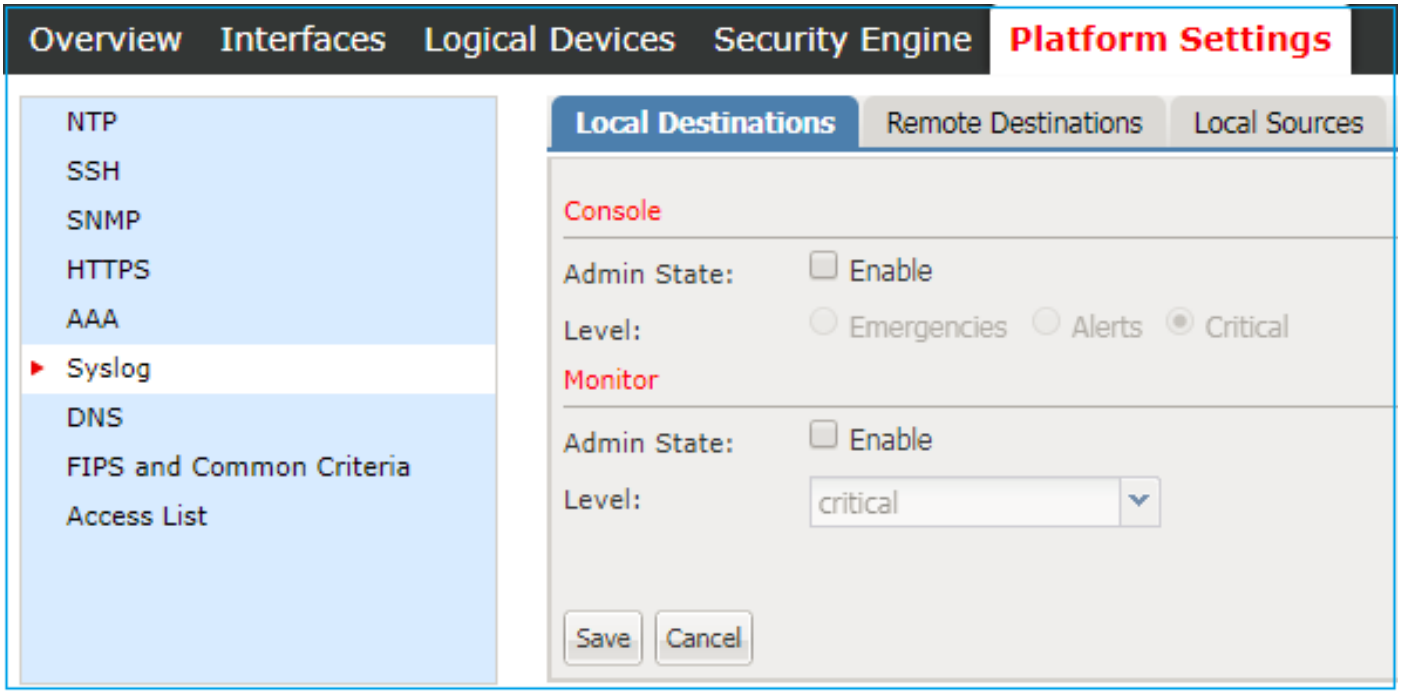
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

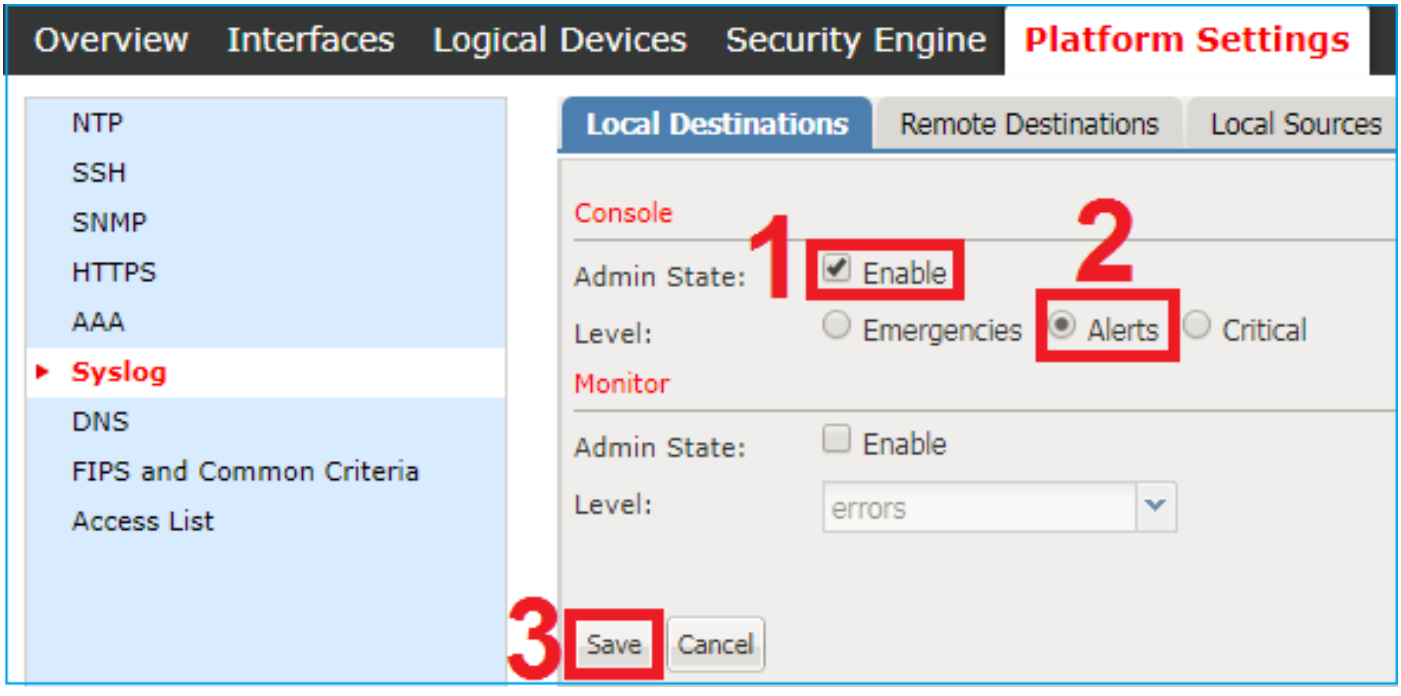
FXOS 사용자 인터페이스에서 Syslog 구성(FPR4100/FPR9300)

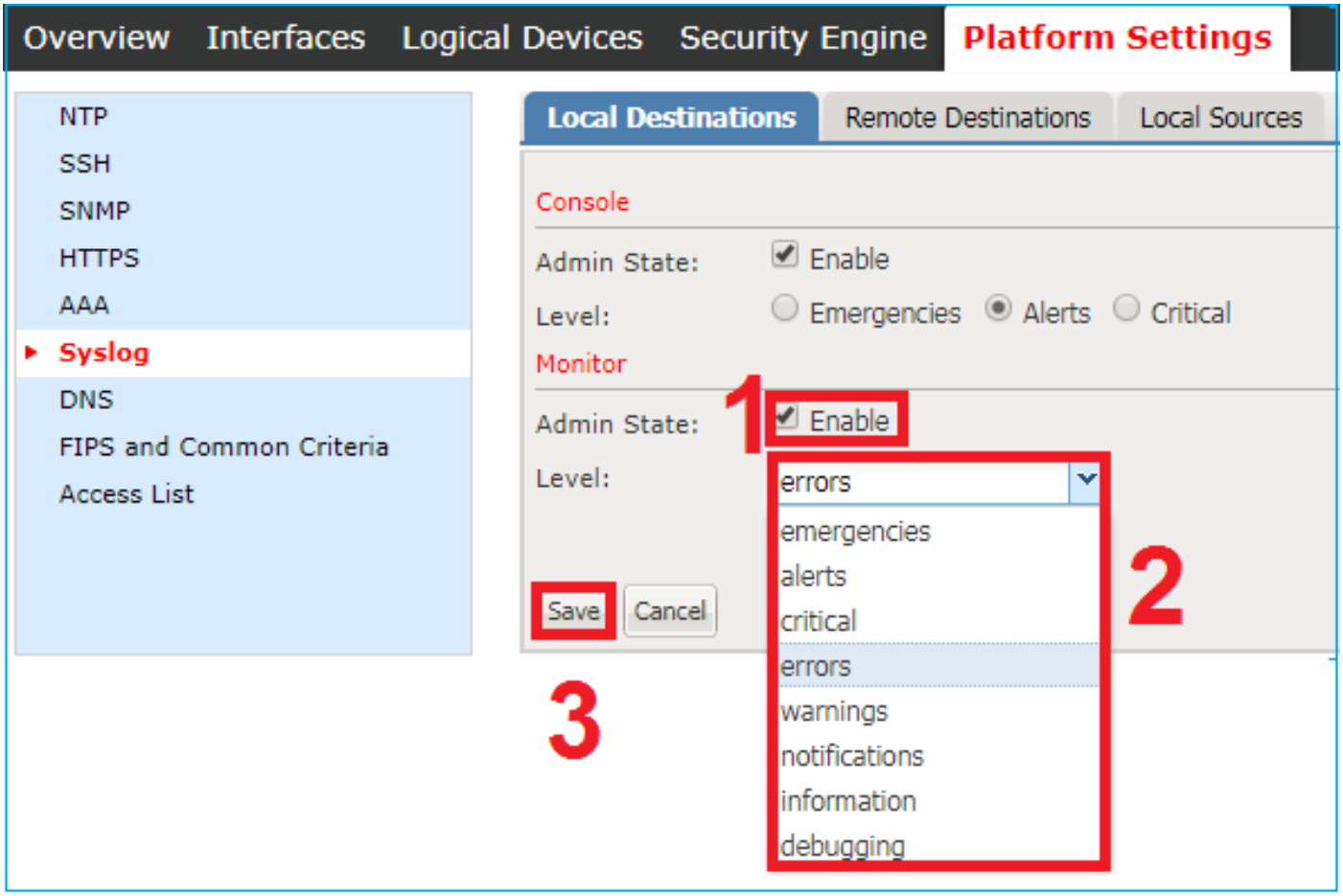
FXOS에는 FCM(Firepower Chassis Manager)에서 활성화하고 구성할 수 있는 자체 Syslog 메시지 집합이 있습니다.

1단계. Platform Settings(**플랫폼 설정**) > **Syslog로 이동합니다.**

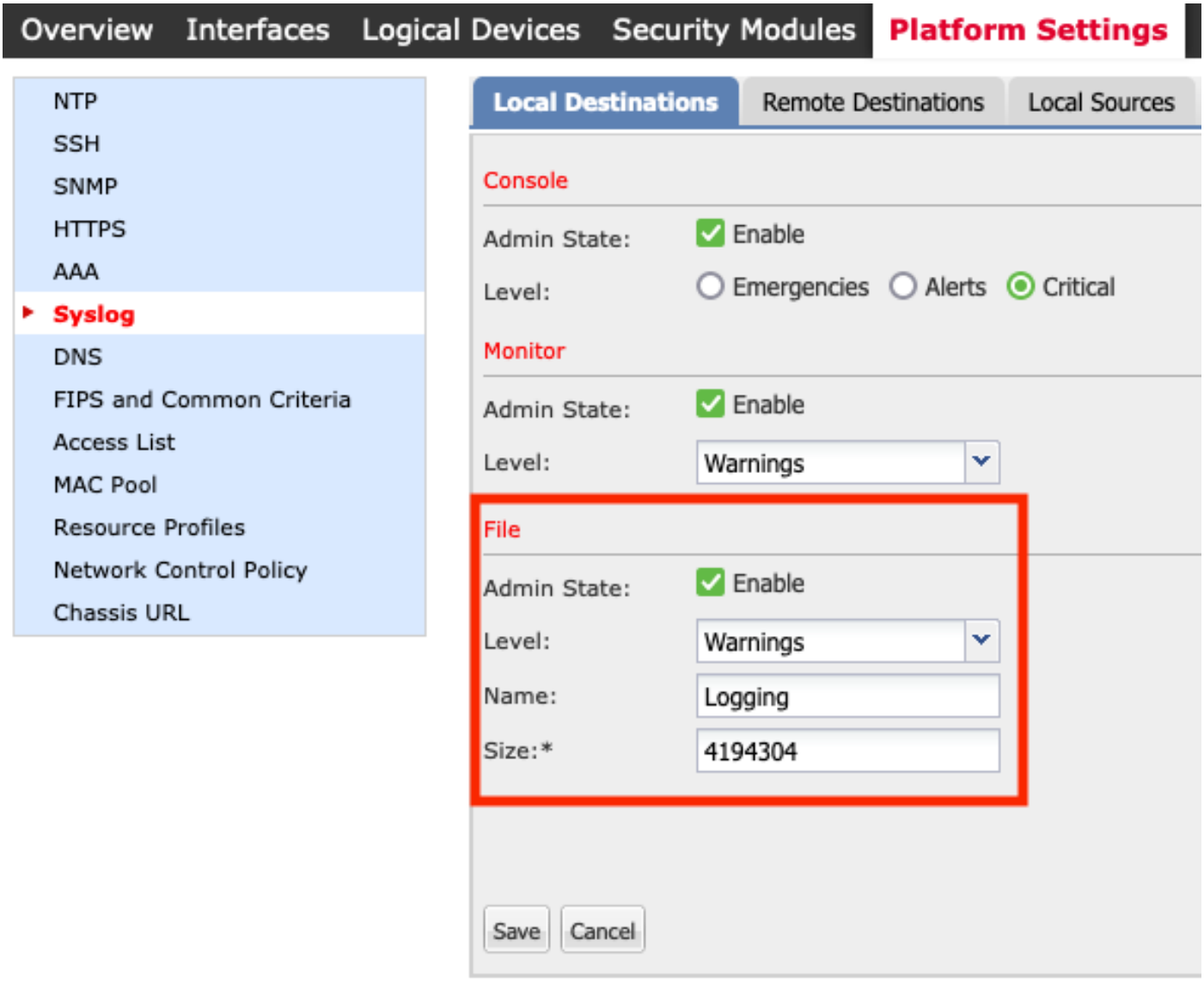


2단계. Local Destinations(**로컬 대상**)에서 로컬로 저장된 모든 레벨에 대해 Syslog의 레벨 0-2 또는 로컬 모니터링에 대해 Syslog 메시지를 활성화할 수 있습니다. 선택한 모든 심각도 레벨도 두 방법 모두에 대해 표시됩니다. 콘솔 및 모니터.





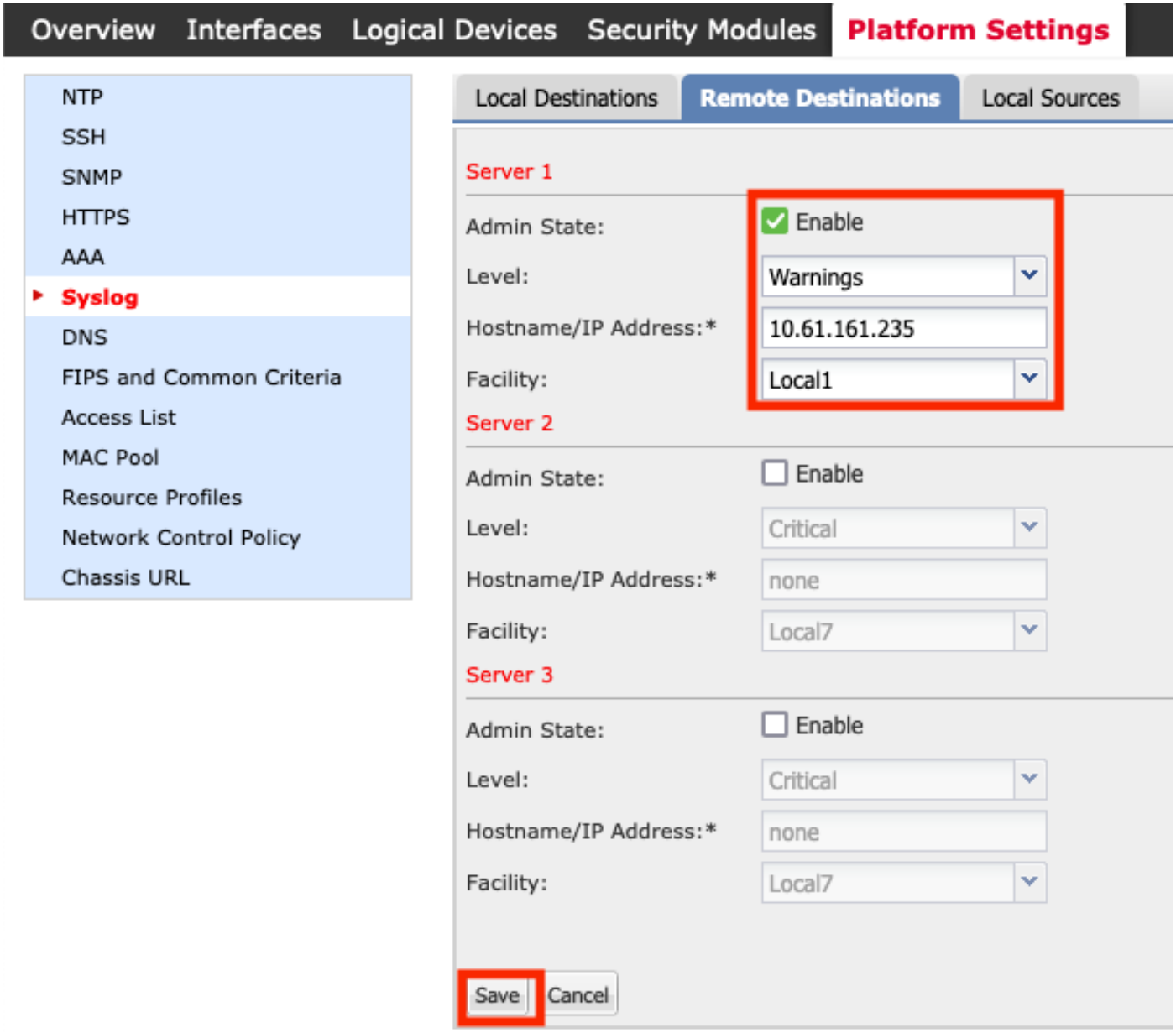
FXOS 버전 2.3.1에서 GUI를 통해 Syslog 메시지에 대한 로컬 파일 대상을 구성할 수도 있습니다.



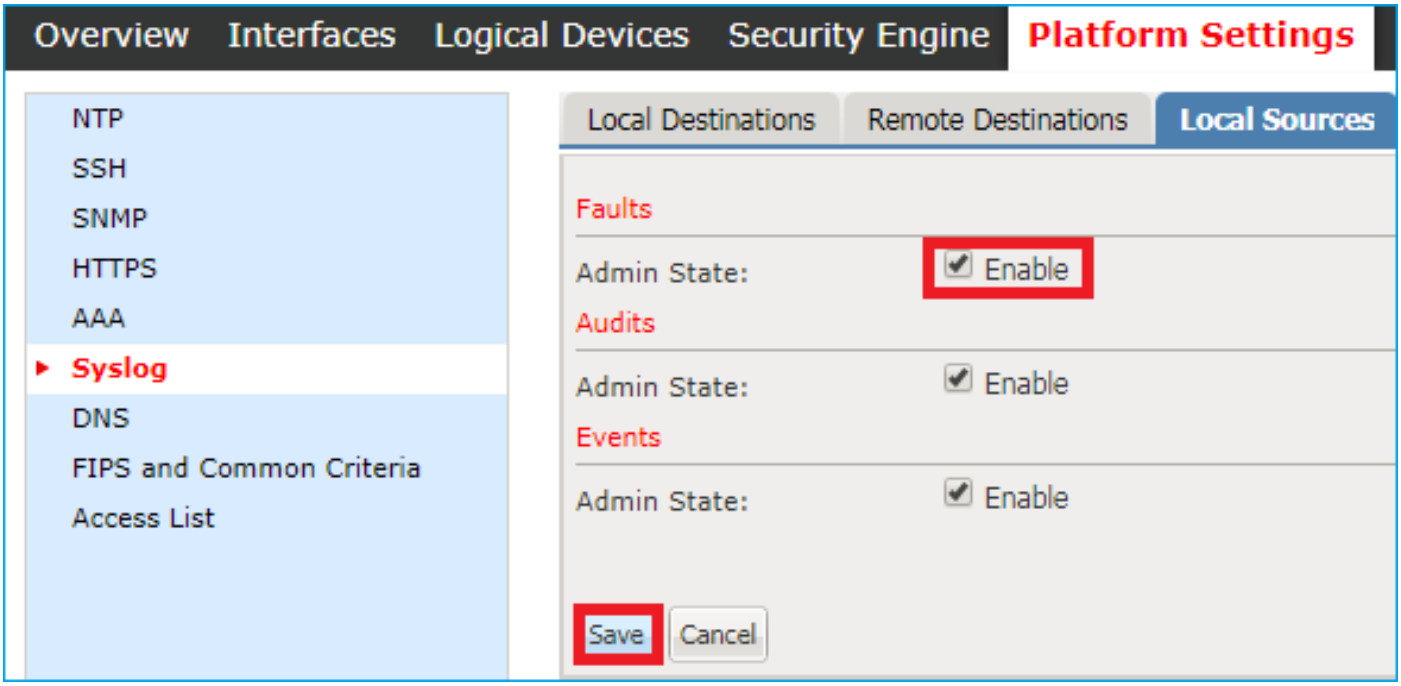
참고: 파일 크기는 4096~4194304바이트 사이만 가질 수 있습니다.

참고: 2.3.1 이전 버전의 FXOS에서는 파일 컨피그레이션을 CLI에서만 사용할 수 있습니다.

Remote Destinations 탭에서 최대 3개의 원격 Syslog 서버를 구성할 수도 있습니다. 각 서버는 서로 다른 Syslog 심각도 수준 메시지의 대상으로 정의되고 다른 로컬 기능으로 플래그 지정될 수 있습니다.



3단계. 마지막으로, Syslog 메시지에 대한 추가 로컬 소스를 선택합니다. FXOS는 Syslog 소스 결함, 감사 메시지 및/또는 이벤트로 사용할 수 있습니다.



FXOS CLI에서 Syslog 구성(FPR4100/FPR9300)

Local Destinations(로컬 대상) 섹션에 해당하는 CLI를 통해 **구성합니다.**

```
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
```

Remote Destinations(**원격 대상**) 섹션에 해당하는 CLI를 통해 **구성합니다**.

```
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
```

Local Sources(로컬 소스) 섹션에 해당하는 CLI를 통해 **구성합니다**.

```
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
```

또한 로컬 파일을 Syslog 대상으로 활성화할 수 있습니다. 다음 Syslog 메시지는 show logging 명령을 사용하거나 logging logfile을 **show logging** 명령을 사용하여 표시할 수 있습니다.

```
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
```

참고: 이 파일의 기본 크기는 최대(4194304바이트)입니다.

CLI를 통해 컨피그레이션 확인

컨피그레이션은 범위 **모니터링**에서 확인 및 구성할 수 있습니다.

```
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
```

또한 **show logging** 명령을 사용하여 FXOS CLI에서 보다 완전한 출력을 얻을 수 있습니다.

```
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]
```

Syslog 메시지가 터미널 모니터 아래에 나타나는지 확인합니다.

Syslog 모니터가 활성화된 경우 모니터 터미널이 활성화된 경우 Syslog 메시지가 FXOS CLI 아래

에 있습니다.

```
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]
```

구성된 원격 호스트에 대한 서비스 확인

Syslog 서버에서 메시지가 수신되었는지 확인합니다.

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

Ethanalyzer 툴을 사용하여 FXOS CLI에서 트래픽을 캡처하여 Syslog 메시지가 생성되어 FXOS에서 전송되는지 확인합니다.

이 예에서는 메시지의 대상이 로컬 Syslog 서버(10.61.161.235), 기능 플래그(Local1) 및 메시지의 심각도(6)와 일치합니다.

```
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]
```

FXOS에서 로컬 로그 파일이 올바르게 로깅되는지 확인합니다.

```
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
```

테스트 Syslog 메시지 생성

또한 CLI를 통해 테스트 목적으로 온디맨드 방식으로 심각도의 Syslog 메시지를 생성하는 옵션도 있습니다. 이렇게 하면 매우 활동적인 Syslog 서버에서 Syslog 메시지가 올바르게 전송되었는지 확인할 수 있도록 보다 구체적인 필터를 정의할 수 있습니다.

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

이 메시지는 모든 Syslog 대상으로 전달되며 특정 Syslog 소스의 필터링이 불가능한 시나리오에서 유용할 수 있습니다.

```
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]

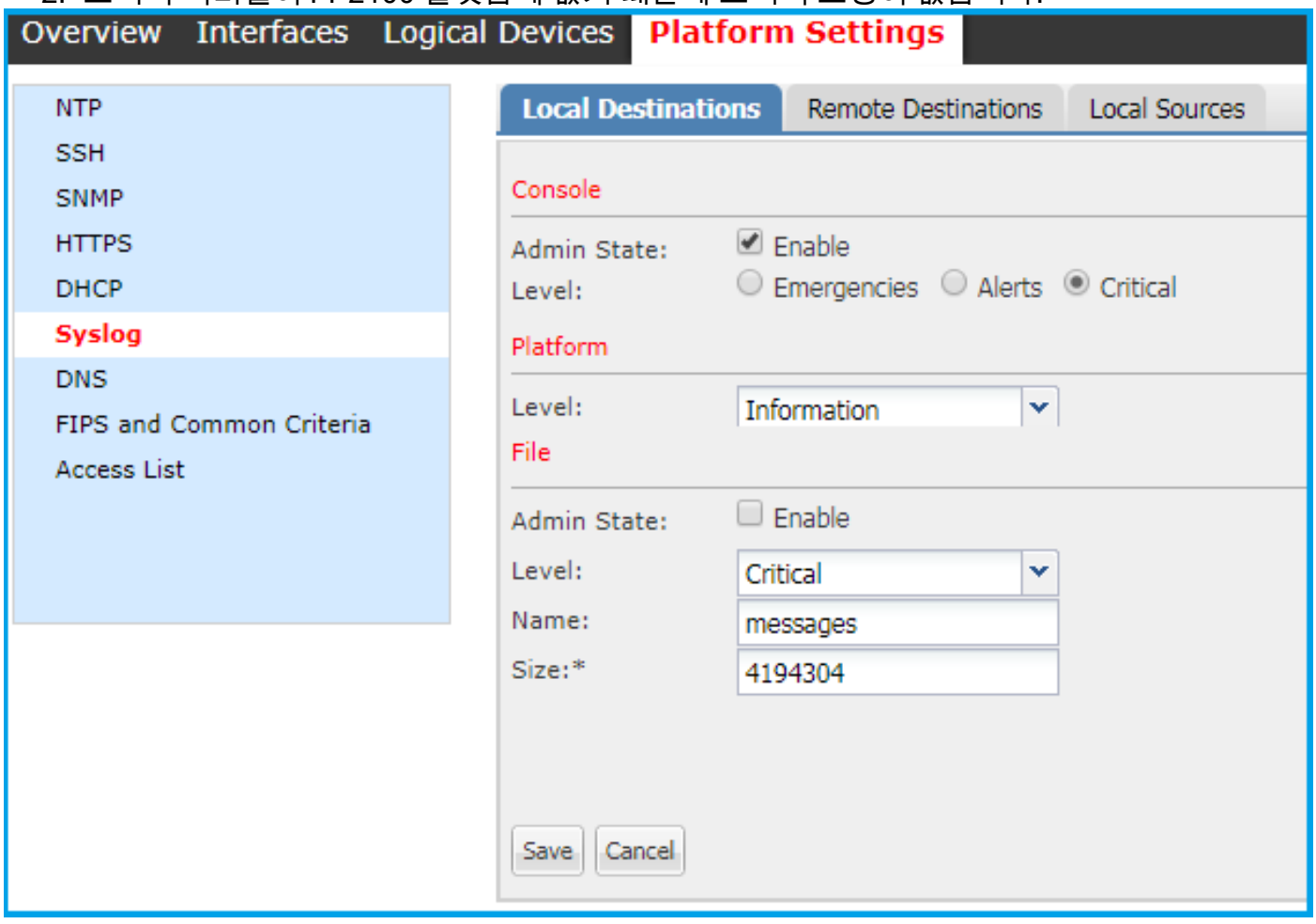
Firepower 2100 어플라이언스의 FXOS Syslog

FPR2100의 ASA 논리적 디바이스

Firepower 4100/9300에 대한 Syslog 컨피그레이션과 ASA 소프트웨어를 사용하는 Firepower 2100 어플라이언스에는 두 가지 주요 차이점이 있습니다.

1. Firepower 2100에서 플랫폼 로깅은 기본적으로 활성화되며 비활성화할 수 없습니다.

2. 모니터 터미널이 FP2100 플랫폼에 없기 때문에 모니터 로깅이 없습니다.



둘 다 **원격 대상** 및 **로컬 소스** 섹션은 다른 플랫폼과 동일합니다.

로그 파일 및 플랫폼 라이브 로그는 CLI 명령을 통해 액세스할 수 없습니다.

FPR2100의 FTD 논리적 디바이스

FTD 어플라이언스가 설치된 FPR2100에서는 다른 토폴로지와 크게 두 가지 차이점이 있습니다.

1. 소스 IP 주소는 논리적 디바이스 Syslog 메시지에 사용된 것과 동일합니다.

2. 모든 FXOS 메시지는 Syslog ID에 사용되며 ASA 199013-199019의 일반 프로세스에 대한 메시지입니다.

```
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
```

이 예에서는 인터페이스 종료 Syslog 메시지가 있습니다.

FAQ

Syslog에서 사용하는 기본 포트는 무엇입니까?

기본적으로 Syslog는 UDP 포트 514를 사용합니다

TCP를 통해 Syslog를 구성할 수 있습니까?

TCP를 통한 Syslog는 FXOS Syslog가 ASA 메시지와 통합된 FTD 어플라이언스가 있는 FPR2100에서만 지원됩니다

관련 정보

- FXOS CLI 컨피그레이션 가이드
- 기술 지원 및 문서 – Cisco Systems