Konfigurieren von Syslog auf FirePOWER FXOS-Appliances

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Syslog auf FirePOWER eXtensible Operating System (FXOS)-Appliances konfiguriert, verifiziert und Fehler behoben werden.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- 1x FPR4120 mit FXOS Softwareversion 2.2(1.70)
- 1 FPR2110 mit ASA Software Version 9.9(2)
- 1x FPR2110 mit FTD-Software, Version 6.2.3
- 1 Syslog-Server

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

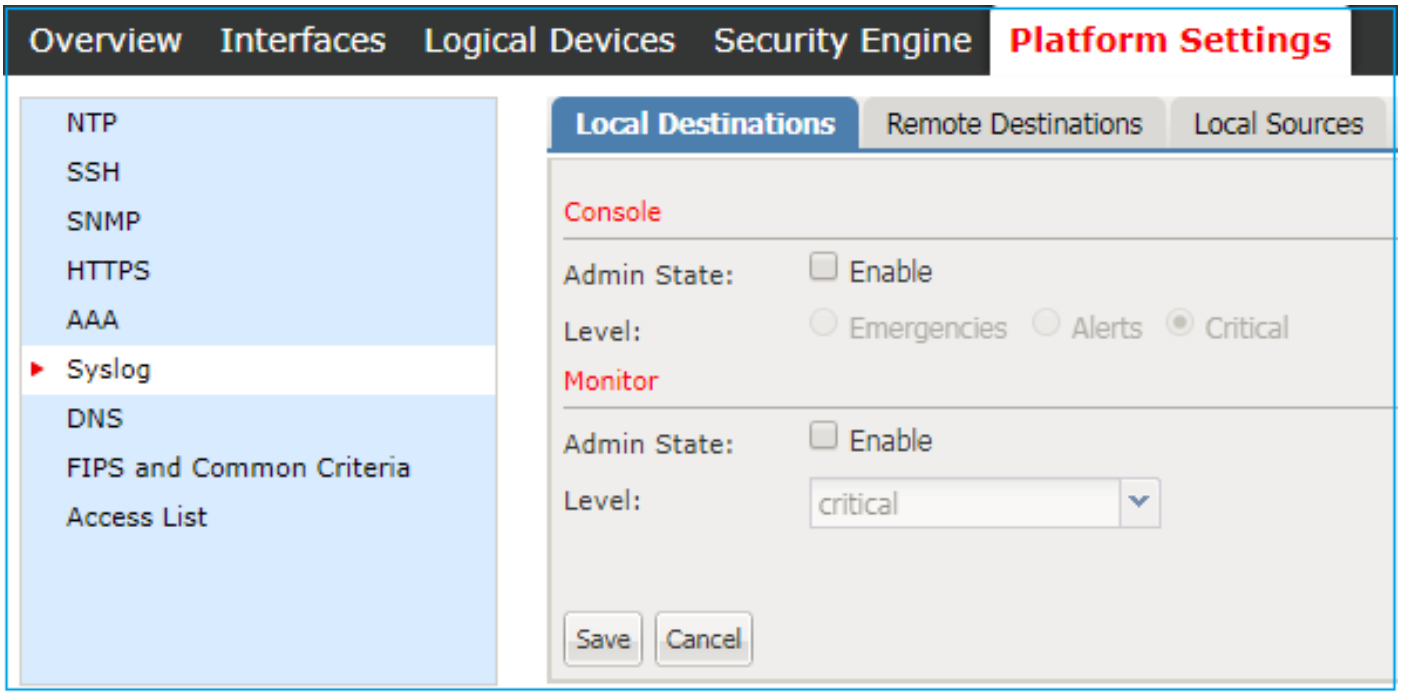
(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

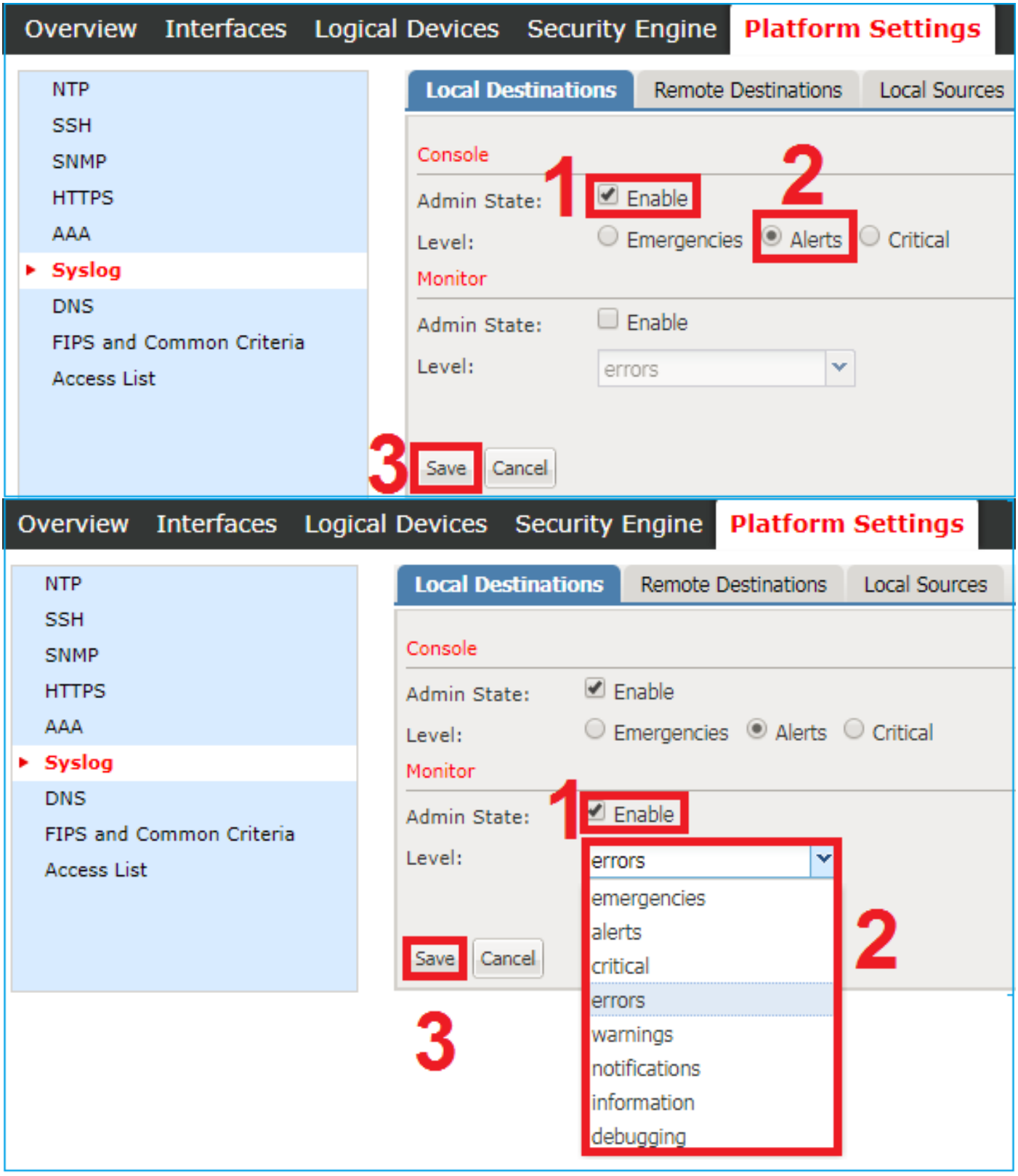
Konfigurieren von Syslog über die FXOS-Benutzeroberfläche (FPR4100/FPR9300)

FXOS verfügt über eigene Syslog-Meldungen, die über den FirePOWER Chassis Manager (FCM) aktiviert und konfiguriert werden können.

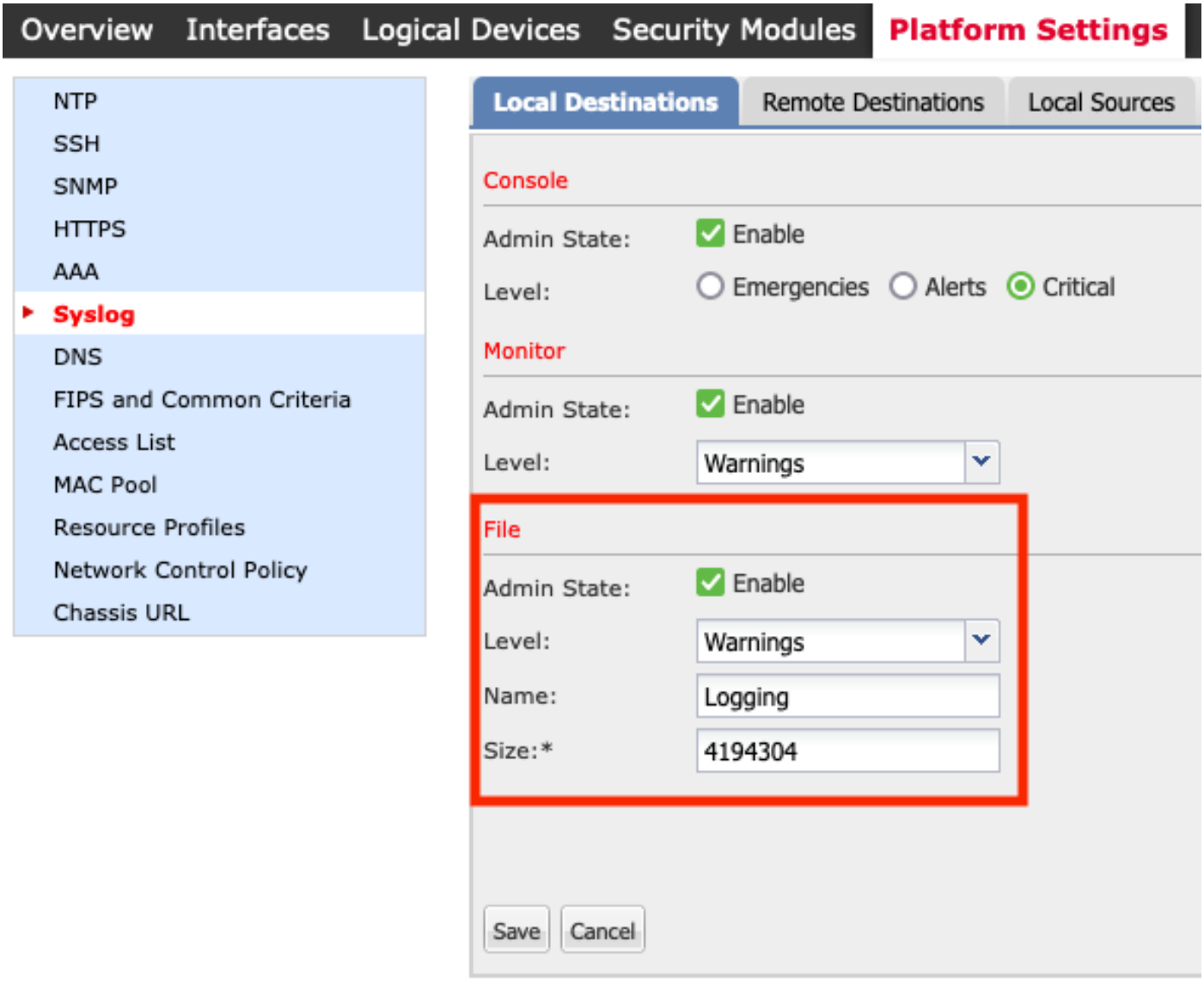
Schritt 1: Navigieren Sie zu **Plattformeinstellungen > Syslog.**



Schritt 2: Unter **Lokale Ziele** können Sie Syslog-Meldungen auf der Konsole für die Ebenen 0-2 oder die lokale Überwachung von Syslog für alle lokal gespeicherten Ebenen aktivieren. Beachten Sie, dass alle über dem ausgewählten liegenden Schweregrade auch für beide Methoden angezeigt werden: Konsole und Monitor.



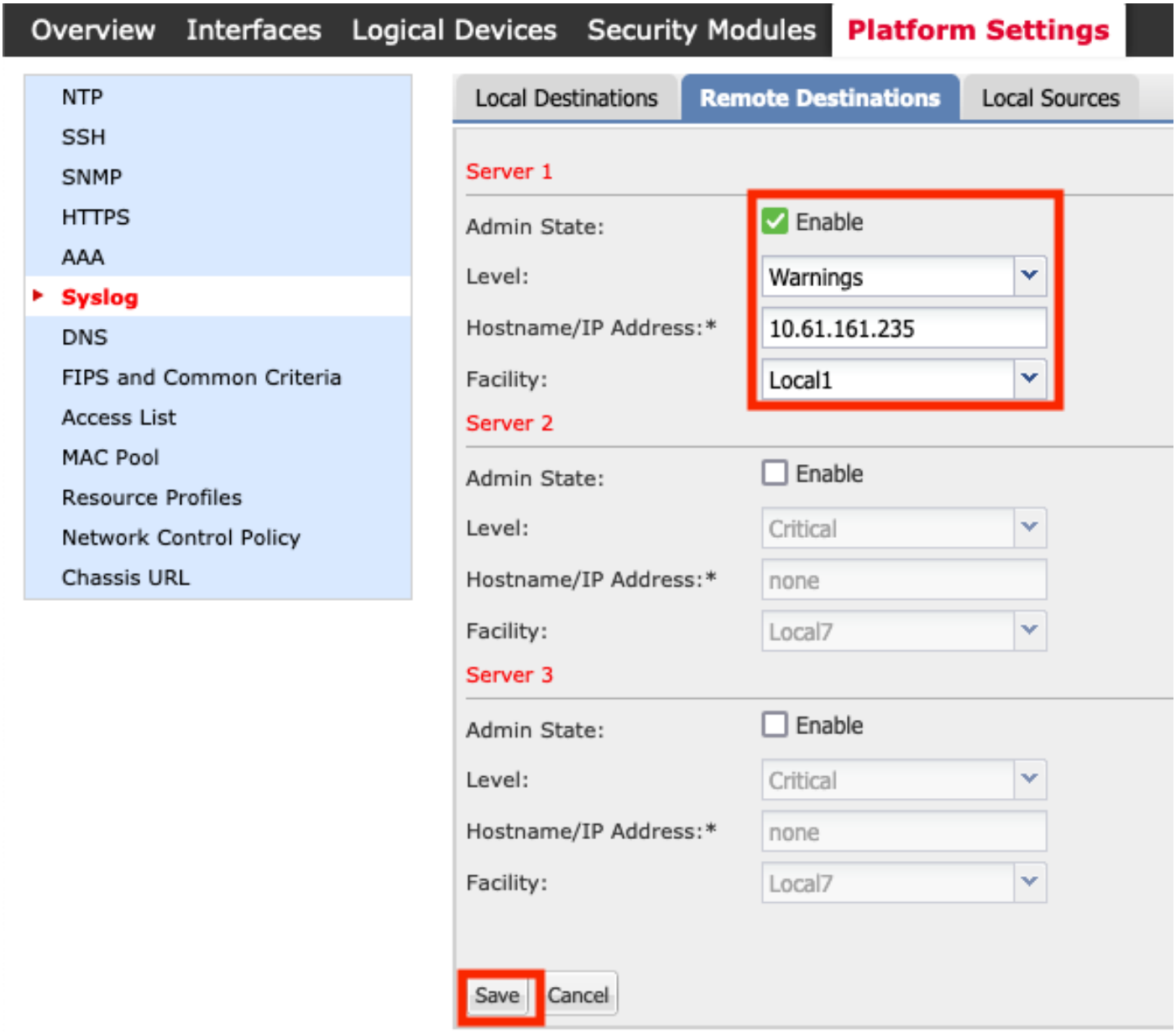
Ab FXOS Version 2.3.1 können Sie über die Benutzeroberfläche auch ein lokales Dateiziel für Syslog-Meldungen konfigurieren:



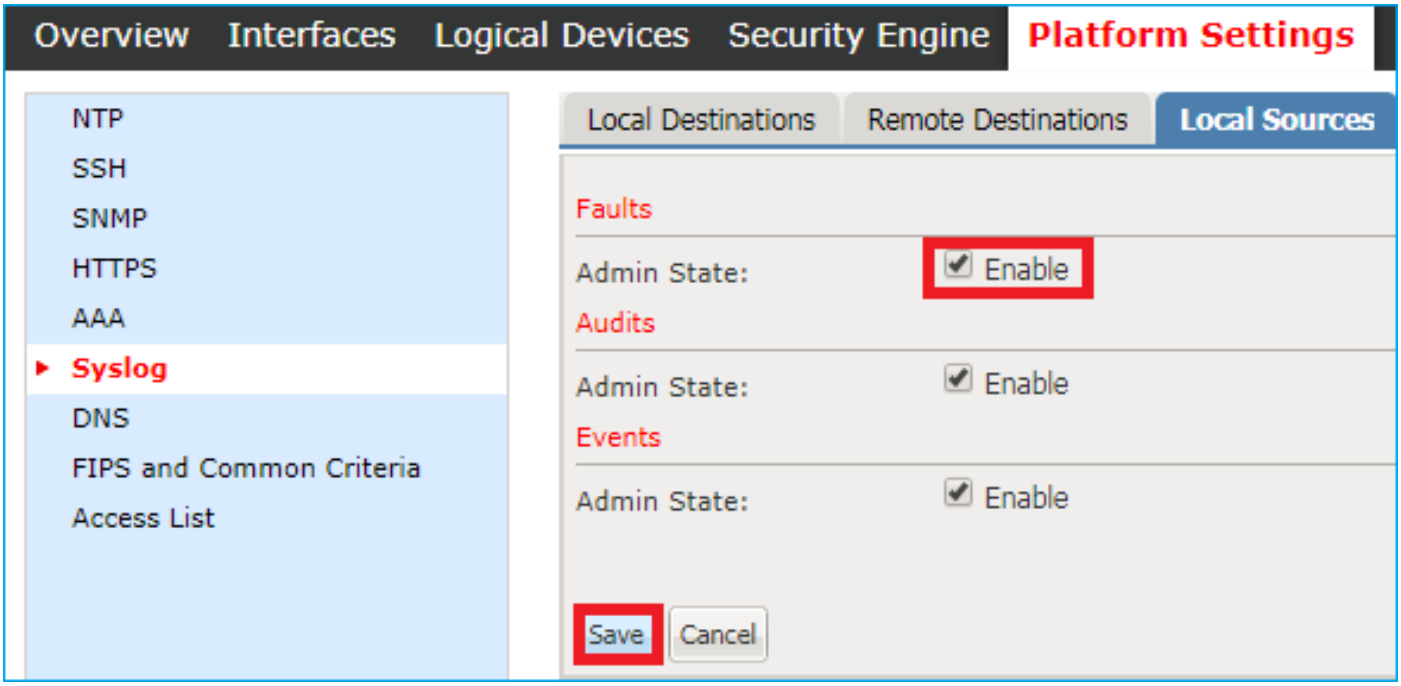
Hinweis: Die Dateigröße kann nur 4096 bis 4194304 Byte groß sein.

Hinweis: In der Version vor 2.3.1 von FXOS ist die Dateikonfiguration nur über CLI verfügbar.

Sie können auch bis zu 3 Syslog-Remote-Server von der Registerkarte **Remote Destorities** konfigurieren. Jeder Server kann als Ziel für verschiedene Syslog-Schweregrad-Meldungen definiert und mit einer anderen lokalen Einrichtung gekennzeichnet werden.



Schritt 3: Wählen Sie schließlich weitere **lokale Quellen** für die Syslog-Meldungen aus. FXOS kann als Syslog-Quelle für Fehler, Überwachungsmeldungen und/oder Ereignisse verwendet werden.



Konfigurieren von Syslog über FXOS CLI (FPR4100/FPR9300)

Konfigurieren Sie über die CLI die Entsprechung des Abschnitts **Lokale Ziele:**

```
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 debugging
FP4120-A /monitoring* # commit-buffer
```

Konfigurieren Sie über die CLI die Entsprechung des Abschnitts **Remote-Ziele**:

```
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 debugging
FP4120-A /monitoring* # set syslog remote-destination server-1 hostname 10.61.161.235
FP4120-A /monitoring* # commit-buffer
```

Konfigurieren Sie über die CLI die Entsprechung des Abschnitts **Lokale Quellen**:

```
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
```

Darüber hinaus können Sie eine lokale Datei als Syslog-Ziel aktivieren. Diese Syslog-Meldungen können mit den Befehlen **show logging** oder **show logging logfile** angezeigt werden:

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

Hinweis: Die Standardgröße dieser Datei ist die maximale Größe (4194304 Byte).

Überprüfen der Konfiguration über die CLI

Die Konfiguration kann über die **Überwachung** des Bereichs überprüft und konfiguriert werden:

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

console
    state: Enabled
    level: Critical

monitor
    state: Enabled
    level: Debugging

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

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

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

Darüber hinaus können Sie mit dem Befehl **show logging** eine vollständigere Ausgabe aus der FXOS-CLI erhalten:

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

Logging console:                enabled (Severity: critical)
Logging monitor:                enabled (Severity: debugging)
Logging linecard:               enabled (Severity: notifications)
Logging fex:            enabled (Severity: notifications)
Logging timestamp:              Seconds
Logging server:                 enabled
{10.61.161.235}
        server severity:        debugging
        server facility:        local1
        server VRF:             management
Logging logfile:                enabled
        Name - Logging: Severity - debugging 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: Testing-Syslog - ucssh[18553]
```

Überprüfen Sie, ob Syslog-Meldungen unter dem Terminalmonitor angezeigt werden.

Wenn der Syslog-Monitor aktiviert ist, sollten Sie Syslog-Meldungen unter der FXOS-CLI sehen, wenn Monitor Terminal aktiviert ist.

```
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]
```

Service für konfigurierte Remote-Hosts überprüfen

Überprüfen Sie, ob Meldungen auf dem Syslog-Server empfangen werden.

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

Erfassen Sie Datenverkehr in der FXOS-CLI mit dem Ethanalyzer-Tool, um zu bestätigen, dass Syslog-Meldungen von FXOS generiert und gesendet werden.

In diesem Beispiel werden das Ziel der Nachricht, die mit dem lokalen Syslog-Server übereinstimmt (10.61.161.235), das Facility-Flag (Local1) und der Schweregrad der Nachricht (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 -> 10.61.161.235 Syslog 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]
```

Überprüfen der ordnungsgemäßen Protokollierung der lokalen Protokolldatei von 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
```

Testen von Syslog-Meldungen generieren

Außerdem besteht die Möglichkeit, Syslog-Meldungen mit einem beliebigen Schweregrad zu Testzwecken über die CLI zu generieren. Auf diese Weise können Sie in sehr aktiven Syslog-Servern einen spezifischeren Filter festlegen, der Ihnen bei der Bestätigung hilft, dass Syslog-Meldungen korrekt gesendet werden:

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

Diese Nachricht wird an jedes Syslog-Ziel weitergeleitet und kann in Szenarien hilfreich sein, in denen das Filtern einer bestimmten Syslog-Quelle nicht möglich ist:

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

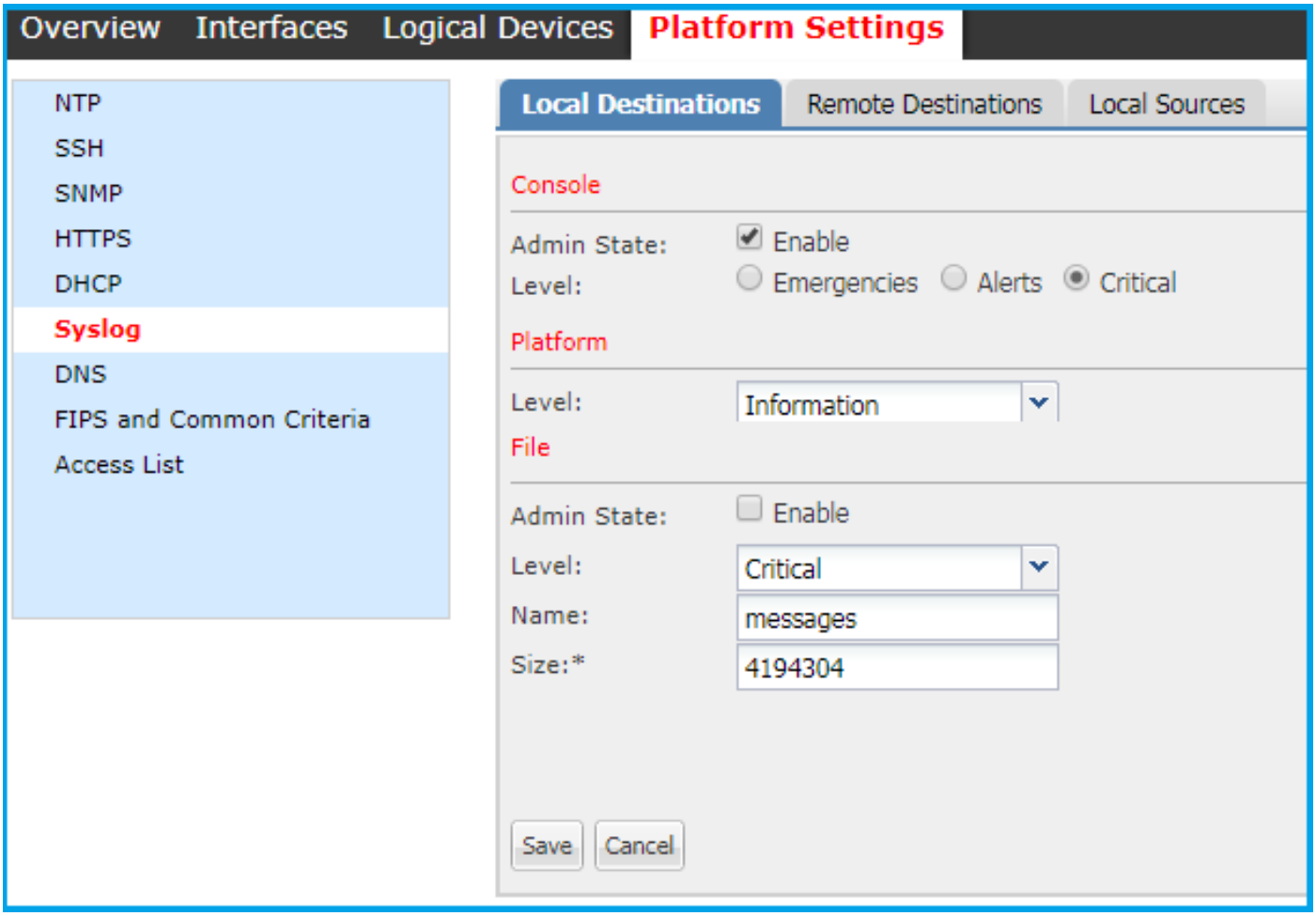
FXOS-Syslog in FirePOWER 2100-Appliances

Logisches ASA-Gerät in FPR2100

Es gibt zwei Hauptunterschiede zwischen der Syslog-Konfiguration für die Firepower 4100/9300- und die Firepower 2100-Appliances mit der ASA-Software.

1. In Firepower 2100 ist die Plattformprotokollierung standardmäßig aktiviert und kann nicht deaktiviert werden.

2. Es wird keine Überwachungsprotokollierung durchgeführt, da das Monitorterminal auf den FP2100-Plattformen nicht vorhanden ist.



Sowohl die Abschnitte **Remote-Ziele** als auch **Lokale Quellen** sind identisch mit den anderen Plattformen.

Auf die Protokolldatei und die Live-Protokolle der Plattform kann nicht über CLI-Befehle zugegriffen werden.

Logisches FTD-Gerät in FPR2100

Bei FPR2100, in dem die FTD-Appliance installiert ist, gibt es im Vergleich zu den anderen Topologien zwei große Unterschiede:

1. Die Quell-IP-Adresse ist die gleiche, die auch für Syslog-Meldungen des logischen Geräts verwendet wird.

2. Alle FXOS-Meldungen werden für die Syslog-ID der Nachricht für die generischen Prozesse der ASA 199013-199019 verwendet.

```
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 diesem Beispiel wird eine Syslog-Meldung über die Schnittstelle heruntergefahren.

Häufig gestellte Fragen

Welcher Standard-Port wird von Syslog verwendet?

Standardmäßig verwendet Syslog den UDP-Port 514

Können Sie Syslog über TCP konfigurieren?

Syslog über TCP wird nur für FPR2100 mit FTD-Appliances unterstützt, bei denen FXOS-Syslogs in die ASA-Nachrichten integriert sind.

Zugehörige Informationen

- Konfigurationsleitfaden für FXOS CLI
- Technischer Support und Dokumentation - Cisco Systems