Configure Syslog on Firepower FXOS Appliances

Contents

Introduction

This document describes how to configure, verify and troubleshoot Syslog on Firepower eXtensible Operating System (FXOS) appliances.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software versions:

- 1x FPR4120 with FXOS software version 2.2(1.70)
- 1x FPR2110 with ASA software version 9.9(2)
- 1x FPR2110 with FTD software version 6.2.3
- 1x Syslog Server

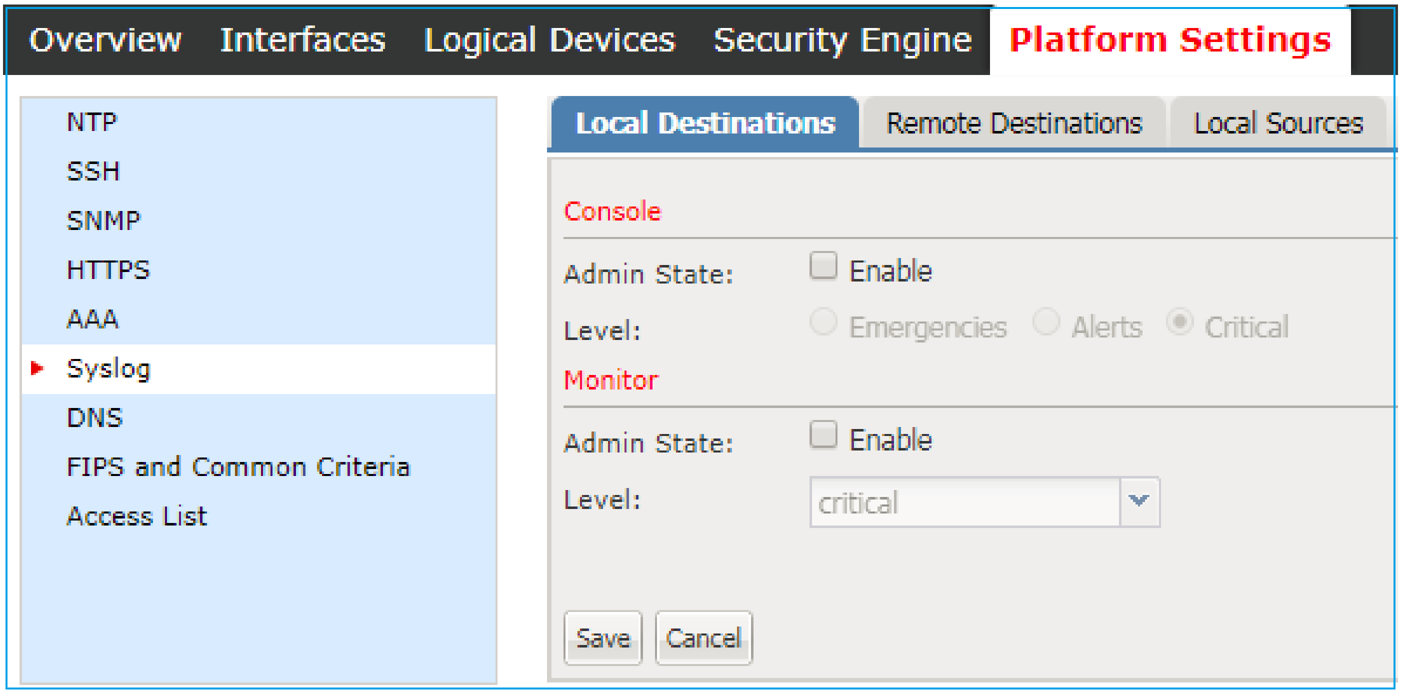
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Configure Syslog from FXOS User Interface (FPR4100/FPR9300)

FXOS has its own set of Syslog messages that can be enabled and configured from the Firepower Chassis Manager (FCM).

Step 1. Navigate to **Platform Settings** > **Syslog.**



Console

Admin State: □ Enable

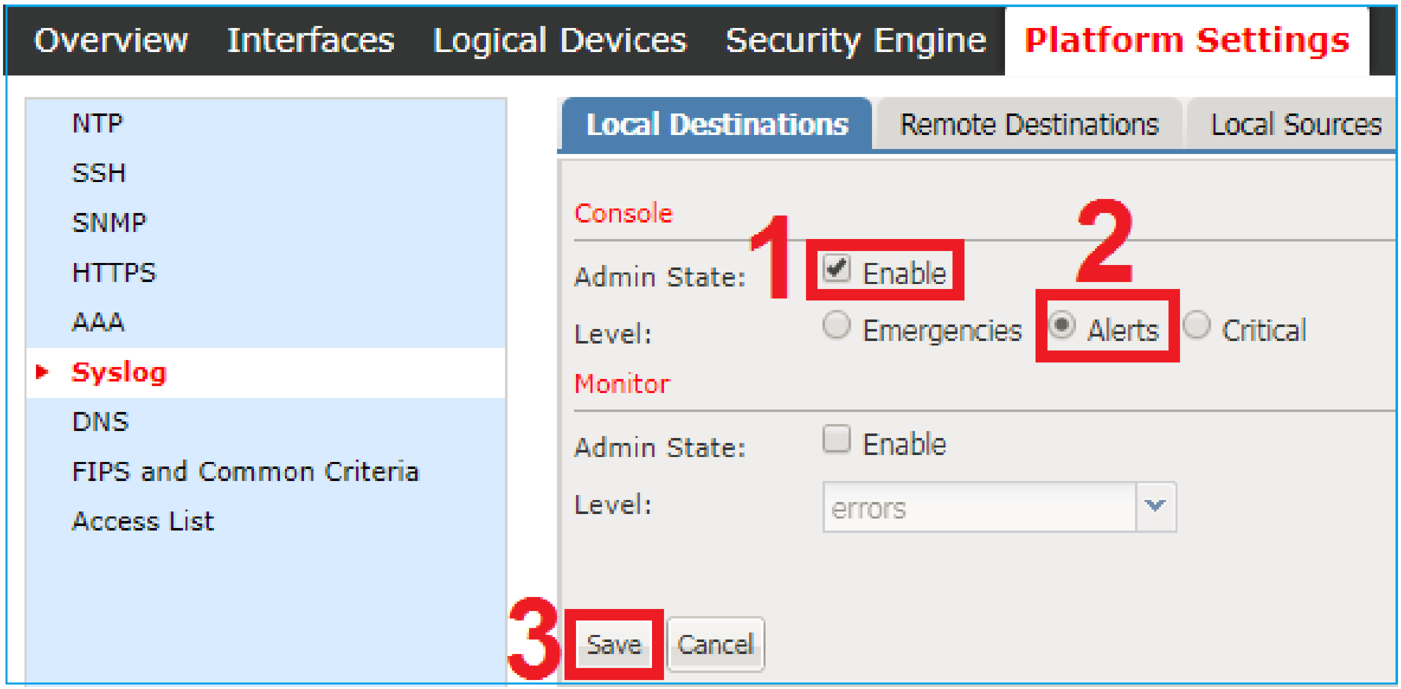
Level: ○ Emergencies ○ Alerts ● Critical

Monitor

Admin State: □ Enable

Level: critical

Step 2. Under **Local Destinations**, you can enable Syslog messages on Console for levels 0-2 or local monitoring of Syslog for any level stored locally. Consider that all the severity levels selected also are displayed for both methods: console and monitor.



Console

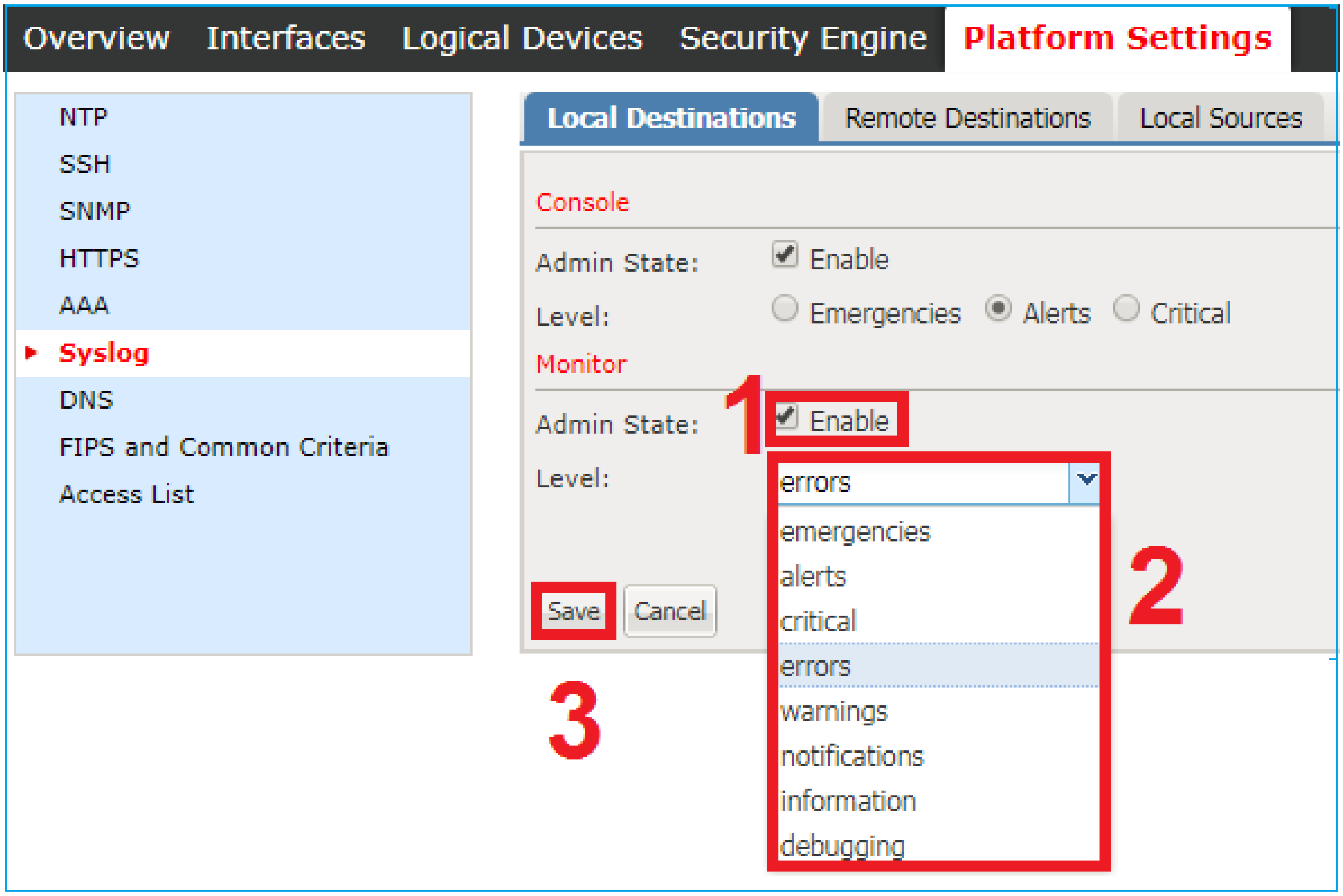
Admin State: ☑ Enable

Level: ○ Emergencies ● Alerts ○ Critical

Monitor

Admin State: □ Enable

Level: errors



Console

Admin State: ☑ Enable

Level: ○ Emergencies ● Alerts ○ Critical

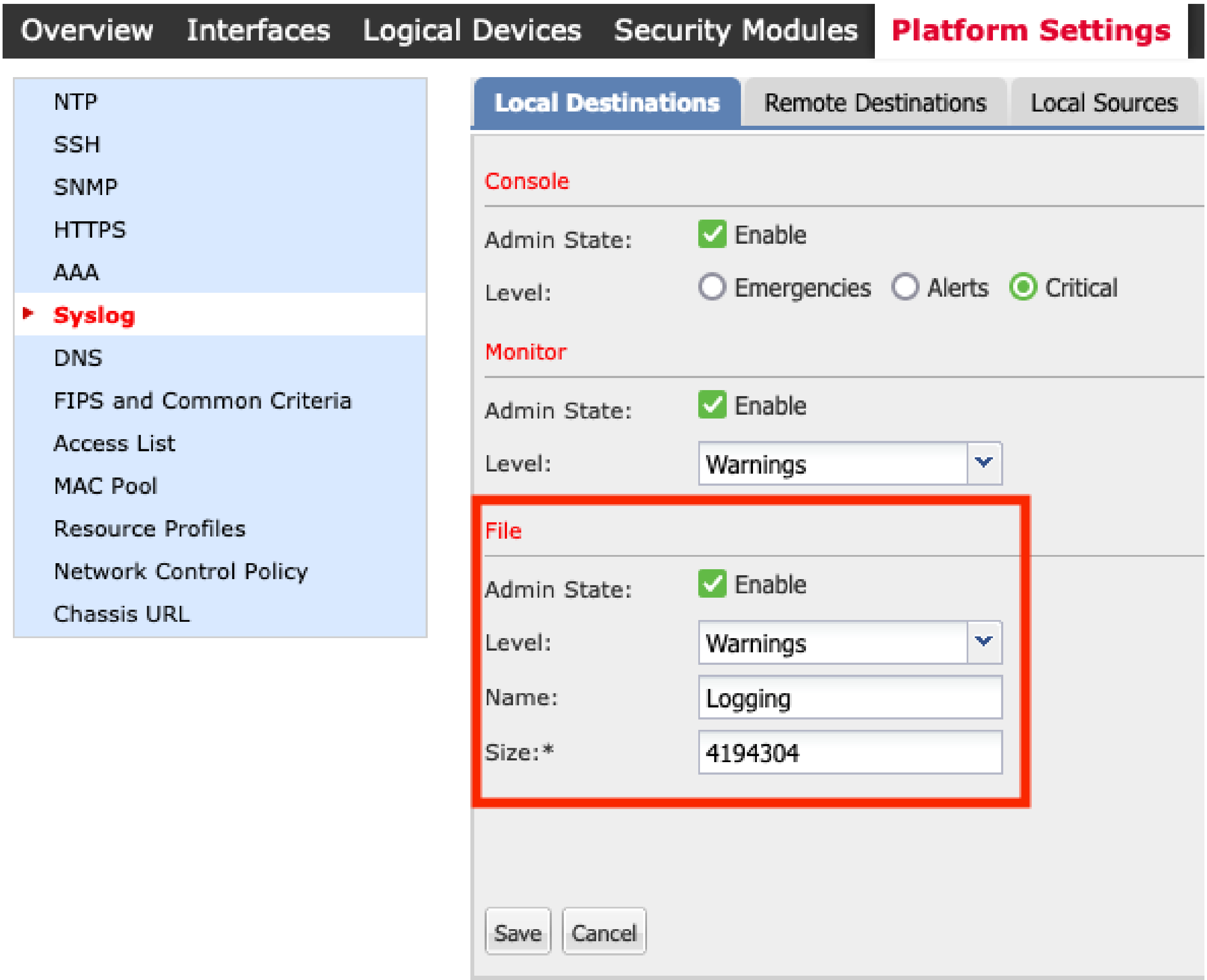
Monitor

Admin State: ☑ Enable

Level: errors

- emergencies
- alerts
- critical
- errors
- warnings
- notifications
- information
- debugging

From FXOS version 2.3.1 you can also configure via GUI a local file destination for Syslog messages:



Console

Admin State: ☑ Enable

Level: ○ Emergencies ○ Alerts ● Critical

Monitor

Admin State: ☑ Enable

Level: Warnings

File

Admin State: ☑ Enable

Level: Warnings

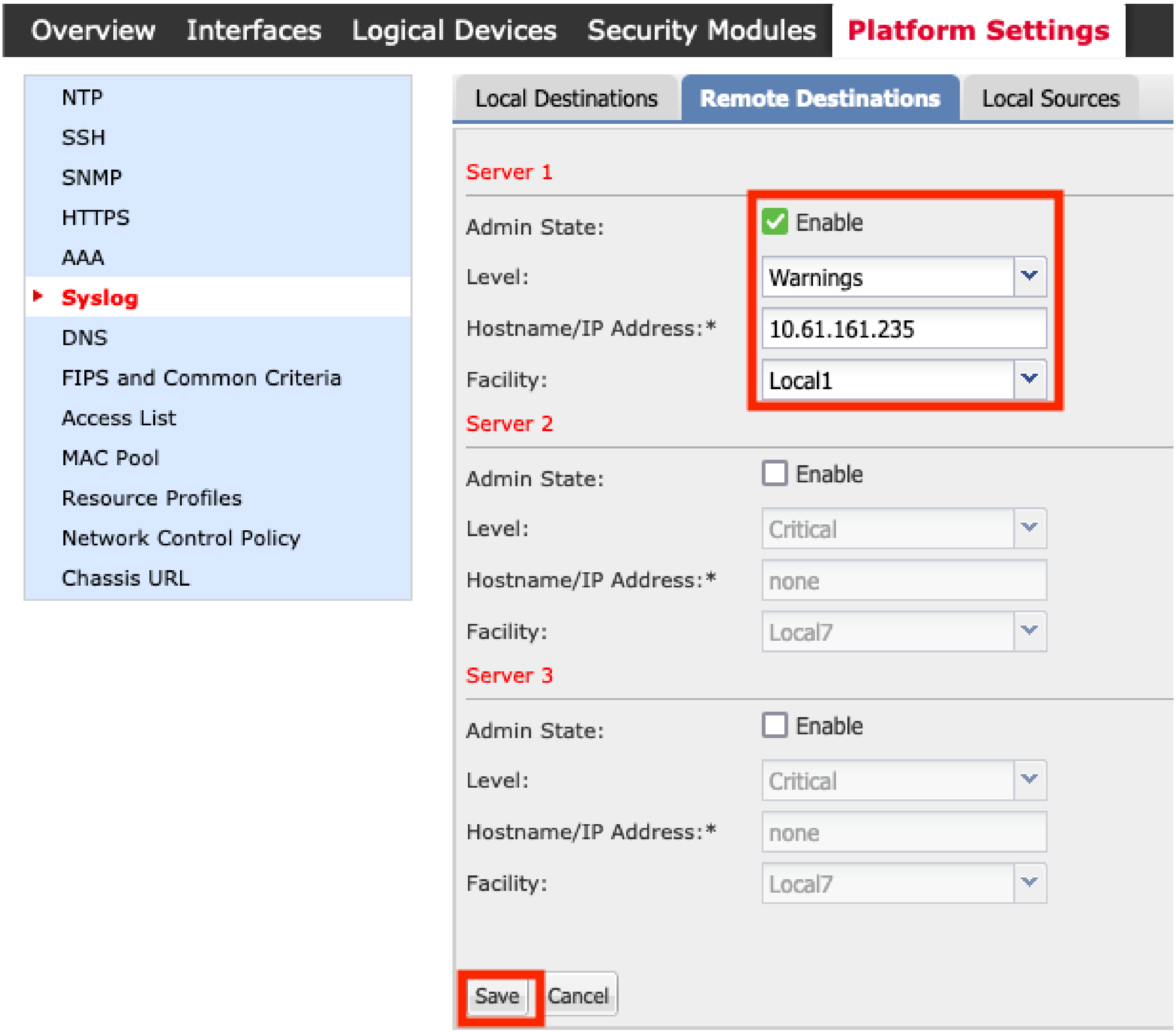
Name: Logging

Size:* 4194304

Note: The file size can only have a size between 4096 and 4194304 bytes.

Note: In pre-2.3.1 FXOS version the File configuration is available via CLI only.

You can also configure up to 3 remote Syslog servers from the **Remote Destinations** tab. Each server can be defined as a destination for different Syslog severity level messages and flagged with a different local facility.



Server 1

Admin State: ☑ Enable

Level: Warnings

Hostname/IP Address:* 10.61.161.235

Facility: Local1

Server 2

Admin State: □ Enable

Level: Critical

Hostname/IP Address:* none

Facility: Local7

Server 3

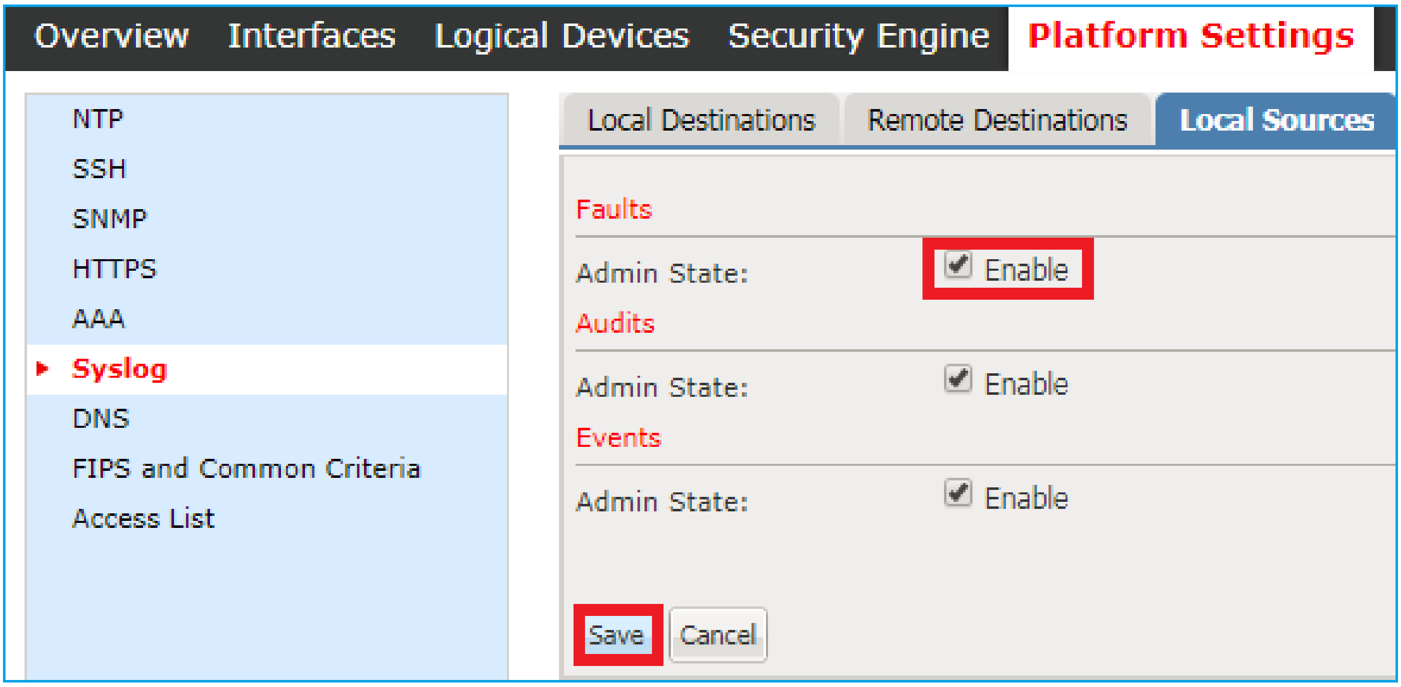
Admin State: □ Enable

Level: Critical

Hostname/IP Address:* none

Facility: Local7

Step 3. Lastly, select additional **Local Sources** for the Syslog messages. FXOS can use as Syslog source Faults, Audit messages and/or Events.



Faults

Admin State: ☑ Enable

Audits

Admin State: ☑ Enable

Events

Admin State: ☑ Enable

Configure Syslog from FXOS CLI (FPR4100/FPR9300)

Configure via CLI the equivalent of section **Local Destinations:**

```
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
```

Configure via CLI the equivalent of section **Remote Destinations**:

```
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
```

Configure via CLI the equivalent of section **Local Sources**:

```
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
```

Additionally, you can enable a local file as a Syslog destination. These Syslog messages can be displayed with the use of the commands **show logging** or **show logging logfile**:

```
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
```

Note: The default size of this file is the maximum (4194304 Bytes).

Verify the Configuration via CLI

The configuration can be verified and configured from scope **monitoring:**

```
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
```

Also, you can get a more complete output from FXOS CLI with the **show logging** command:

```
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]
```

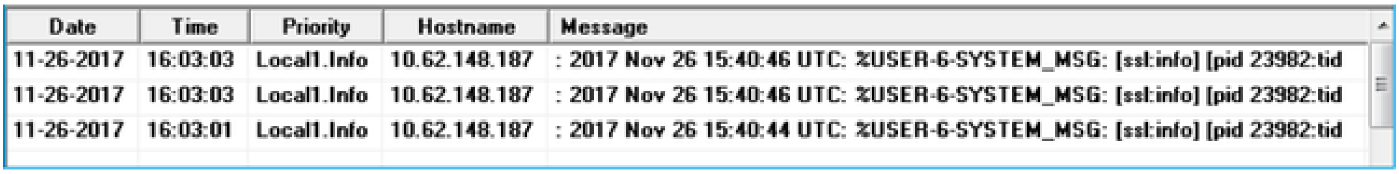
Verify that Syslog Messages Appear under the Terminal Monitor

When Syslog monitor is enabled, Syslog messages are under FXOS CLI when monitor terminal is enabled.

```
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]
```

Verify Service for the Remote Hosts Configured

Verify that messages are received on the Syslog server.



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

Capture traffic on FXOS CLI with the Ethanalyzer tool to confirm that Syslog messages are generated and sent by FXOS.

In this example, the destination of the message match the local Syslog Server (10.61.161.235), the facility flag (Local1) and the severity of the message (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]
```

Verify that Local Log File is Correctly Logging from 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
```

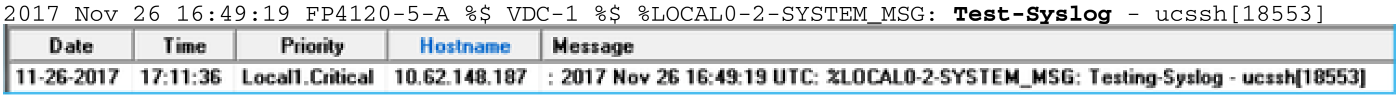
Generate test Syslog Messages

There is also the option to generate Syslog messages of any severity on demand for test purposes via CLI. This way, in very active Syslog servers you can define a more specific filter to assist you to confirm that Syslog messages are correctly sent:

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

This message is forwarded to any Syslog destination and can be helpful in scenarios where filtering of a specific Syslog source is not feasible:

```
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]

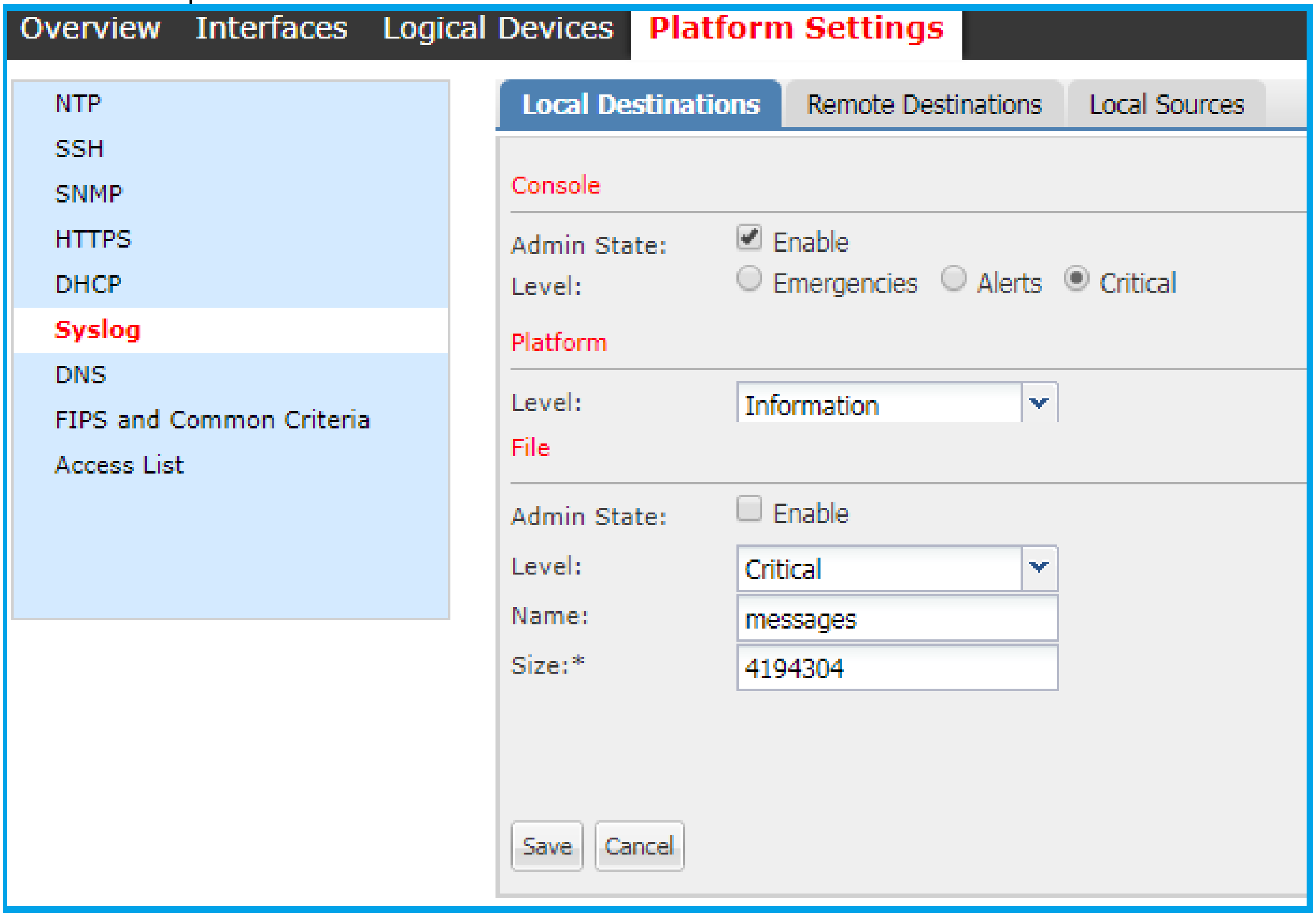
FXOS Syslog in Firepower 2100 Appliances

ASA Logical Device in FPR2100

There are two main differences between Syslog configuration for Firepower 4100/9300 and Firepower 2100 appliances with ASA software.

1. In Firepower 2100 the platform logging is enabled by default and cannot be disabled.

2. There is no monitor logging due to the fact that the monitor terminal does not exist in FP2100 platforms.



Console

Admin State: ☑ Enable

Level: ○ Emergencies ○ Alerts ● Critical

Platform

Level: Information

File

Admin State: □ Enable

Level: Critical

Name: messages

Size:* 4194304

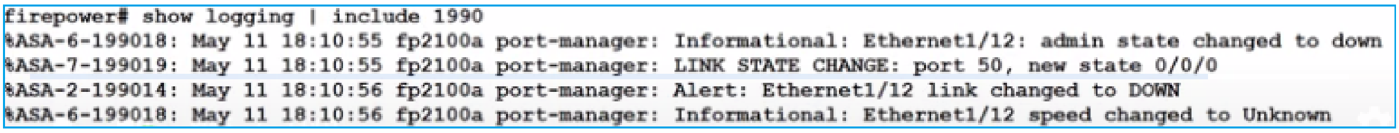
Both, **Remote Destinations** and **Local Sources** sections are identical to the other platforms.

The log file and platform live logs are not accessible via CLI commands.

FTD logical device in FPR2100

In FPR2100 where FTD appliance is installed there are 2 major differences compared with the other topologies:

1. The source IP address is the same that used for the logical device Syslog messages.
2. All FXOS messages are used for Syslog ID the message for generic processes of ASA 199013-199019



```
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 this example, there is the interface shutdown Syslog messages.

FAQ

Which is the default port used by Syslog?

By default, Syslog uses UDP port 514

Can you configure Syslog via TCP?

Syslog via TCP is only supported for FPR2100 with FTD appliances where FXOS Syslogs are integrated with the ASA messages

Related Information

- **FXOS CLI Configuration guide**
- **Technical Support & Documentation - Cisco Systems**