

Configurar Syslog em Dispositivos Firepower FXOS

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configurar Syslog a partir da interface de usuário FXOS \(FPR4100/FPR9300\)](#)

[Configurar Syslog a partir da CLI do FXOS \(FPR4100/FPR9300\)](#)

[Verifique a configuração via CLI](#)

[Verifique se as mensagens de syslog são exibidas sob o Terminal Monitor](#)

[Verificar o serviço dos hosts remotos configurados](#)

[Verifique se o arquivo de log local está fazendo o login correto do FXOS](#)

[Gerar mensagens de syslog de teste](#)

[Syslog FXOS em dispositivos Firepower 2100](#)

[Dispositivo lógico ASA em FPR2100](#)

[Dispositivo lógico FTD em FPR2100](#)

[FAQ](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar, verificar e solucionar problemas de Syslog em dispositivos FXOS (Firepower eXtensible Operating System).

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- 1x FPR4120 com software FXOS versão 2.2(1.70)
- 1x FPR2110 com software ASA versão 9.9(2)
- 1x FPR2110 com software FTD versão 6.2.3
- 1x Servidor Syslog

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. Se a rede estiver

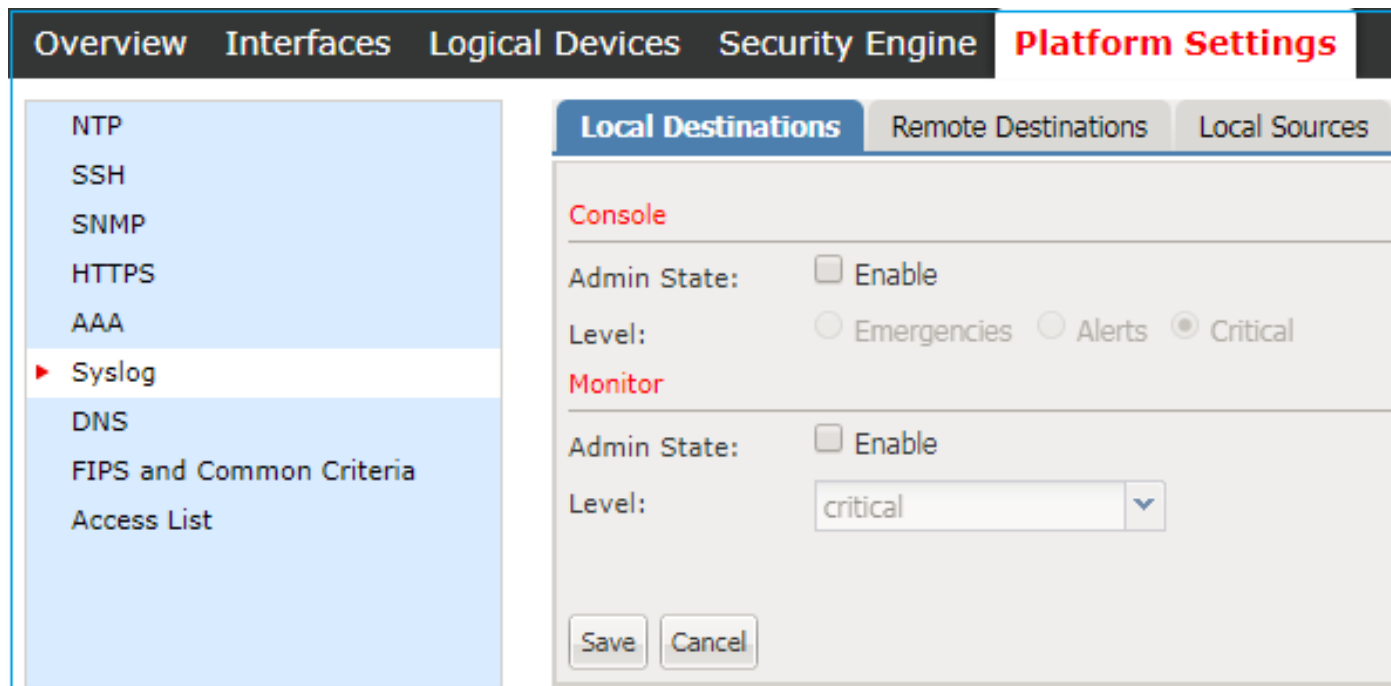
ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Configurar Syslog a partir da interface de usuário FXOS (FPR4100/FPR9300)

O FXOS tem seu próprio conjunto de mensagens Syslog que podem ser ativadas e configuradas no Firepower Chassis Manager (FCM).

Etapa 1. Navegue até **Configurações da plataforma > Syslog**.



The screenshot shows the 'Platform Settings' page in the FXOS interface. The left sidebar contains a menu with options: NTP, SSH, SNMP, HTTPS, AAA, Syslog (selected), DNS, FIPS and Common Criteria, and Access List. The main content area is titled 'Local Destinations' and has three tabs: 'Local Destinations', 'Remote Destinations', and 'Local Sources'. Under the 'Local Destinations' tab, there are two sections: 'Console' and 'Monitor'. The 'Console' section has 'Admin State' set to 'Enable' (checkbox checked) and 'Level' set to 'Critical' (radio button selected). The 'Monitor' section has 'Admin State' set to 'Enable' (checkbox checked) and 'Level' set to 'critical' (dropdown menu). At the bottom of the configuration area are 'Save' and 'Cancel' buttons.

Etapa 2. Em **Destinos locais**, você pode habilitar as mensagens de Syslog no Console para os níveis 0-2 ou monitoramento local do Syslog para qualquer nível armazenado localmente. Considere que todos os níveis de gravidade selecionados também são exibidos para ambos os métodos: console e monitor.

Overview Interfaces Logical Devices Security Engine **Platform Settings**

NTP
SSH
SNMP
HTTPS
AAA
► **Syslog**
DNS
FIPS and Common Criteria
Access List

Local Destinations Remote Destinations Local Sources

Console

Admin State: **1** Enable

Level: Emergencies **2** Alerts Critical

Monitor

Admin State: Enable

Level: errors

3 Save Cancel

Overview Interfaces Logical Devices Security Engine **Platform Settings**

NTP
SSH
SNMP
HTTPS
AAA
► **Syslog**
DNS
FIPS and Common Criteria
Access List

Local Destinations Remote Destinations Local Sources

Console

Admin State: Enable

Level: Emergencies Alerts Critical

Monitor

Admin State: **1** Enable

Level: errors

errors
emergencies
alerts
critical
errors
warnings
notifications
information
debugging

Save Cancel **2**

3

No FXOS versão 2.3.1, você também pode configurar através da GUI um destino de arquivo local para mensagens de Syslog:

- NTP
- SSH
- SNMP
- HTTPS
- AAA
- Syslog**
- DNS
- FIPS and Common Criteria
- Access List
- MAC Pool
- Resource Profiles
- Network Control Policy
- Chassis URL

Local Destinations
Remote Destinations
Local Sources

Console

Admin State: Enable

Level: Emergencies Alerts Critical

Monitor

Admin State: Enable

Level:

File

Admin State: Enable

Level:

Name:

Size: *

Note: O tamanho do arquivo só pode ter um tamanho entre 4096 e 4194304 bytes.

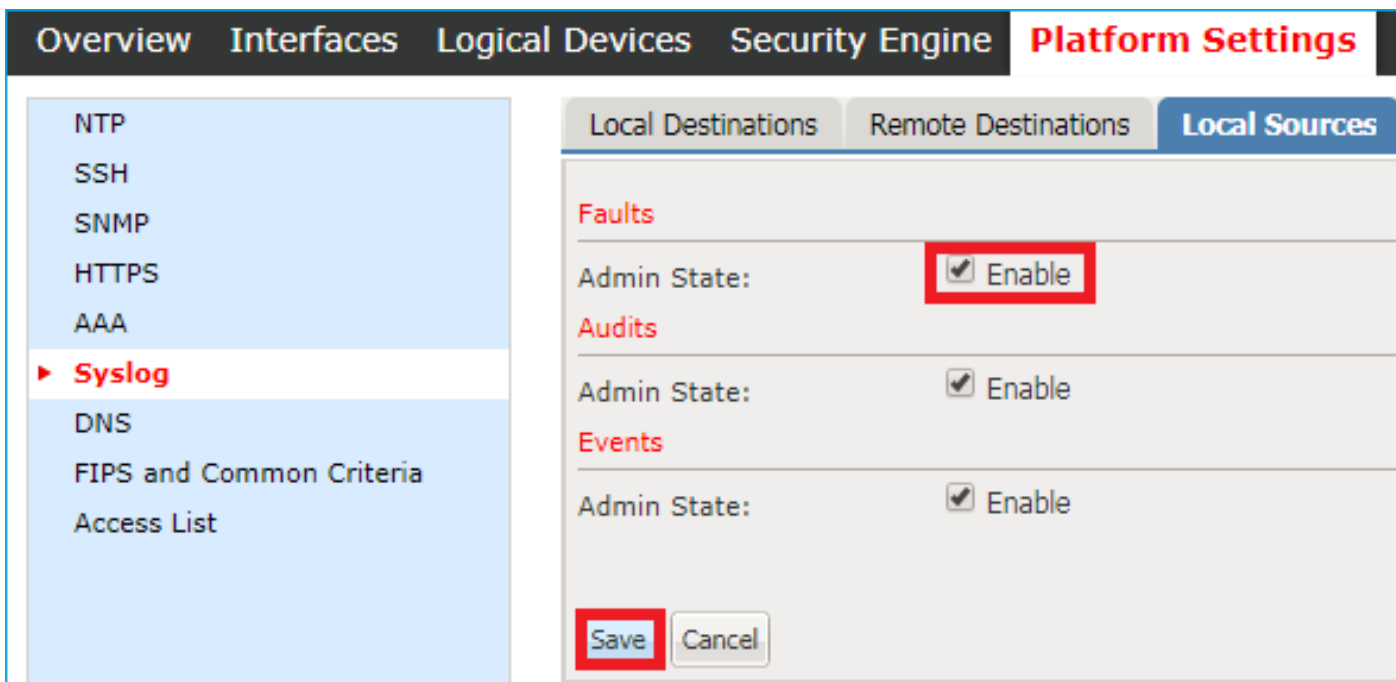
Note: Na versão FXOS anterior à 2.3.1, a configuração do arquivo está disponível somente via CLI.

Você também pode configurar até 3 servidores Syslog remotos na guia **Destinos remotos**. Cada servidor pode ser definido como um destino para mensagens de nível de gravidade Syslog diferentes e sinalizado com uma instalação local diferente.

- NTP
- SSH
- SNMP
- HTTPS
- AAA
- **Syslog**
- DNS
- FIPS and Common Criteria
- Access List
- MAC Pool
- Resource Profiles
- Network Control Policy
- Chassis URL

Local Destinations	Remote Destinations	Local Sources
Server 1		
Admin State:	<input checked="" type="checkbox"/> Enable	
Level:	Warnings	
Hostname/IP Address:*	10.61.161.235	
Facility:	Local1	
Server 2		
Admin State:	<input type="checkbox"/> Enable	
Level:	Critical	
Hostname/IP Address:*	none	
Facility:	Local7	
Server 3		
Admin State:	<input type="checkbox"/> Enable	
Level:	Critical	
Hostname/IP Address:*	none	
Facility:	Local7	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

Etapa 3. Por fim, selecione **Fontes locais** adicionais para as mensagens de Syslog. O FXOS pode usar como fonte de Syslog Falhas, Mensagens de auditoria e/ou Eventos.



Configurar Syslog a partir da CLI do FXOS (FPR4100/FPR9300)

Configure via CLI o equivalente da seção **Destinos locais**:

```
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 por CLI o equivalente da seção **Destinos remotos**:

```
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 o equivalente da seção **Fontes locais**:

```
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
```

Além disso, você pode habilitar um arquivo local como um destino Syslog. Essas mensagens de Syslog podem ser exibidas com o uso dos comandos **show logging** ou **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: O tamanho padrão desse arquivo é o máximo (4194304 bytes).

Verifique a configuração via CLI

A configuração pode ser verificada e configurada a partir do **monitoramento** do escopo:

```
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
```

Além disso, você pode obter uma saída mais completa da CLI do FXOS com o comando **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
mrrib	5	7
misp	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]

Verifique se as mensagens de syslog são exibidas sob o Terminal Monitor

Quando o monitor Syslog está ativado, as mensagens Syslog estão na CLI FXOS quando o terminal de monitor está ativado.

```
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]
```

Verificar o serviço dos hosts remotos configurados

Verifique se as mensagens são recebidas no servidor Syslog.

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 o tráfego na CLI FXOS com a ferramenta Ethalyzer para confirmar se as mensagens Syslog são geradas e enviadas pelo FXOS.

Neste exemplo, o destino da mensagem corresponde ao Servidor Syslog local (10.61.161.235), ao sinalizador de recurso (Local1) e à gravidade da mensagem (6):

```
FP4120-A(fxos)# ethalyzer 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]
```

Verifique se o arquivo de log local está fazendo o login correto do 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
```

Gerar mensagens de syslog de teste

Também há a opção de gerar mensagens Syslog de qualquer gravidade sob demanda para fins de teste via CLI. Dessa forma, em servidores Syslog muito ativos, você pode definir um filtro mais específico para ajudá-lo a confirmar se as mensagens Syslog foram enviadas corretamente:

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

Esta mensagem é encaminhada para qualquer destino de Syslog e pode ser útil em cenários em que a filtragem de uma fonte de Syslog específica não é viável:

```
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]

Syslog FXOS em dispositivos Firepower 2100

Dispositivo lógico ASA em FPR2100

Há duas diferenças principais entre a configuração do Syslog para dispositivos Firepower 4100/9300 e Firepower 2100 com software ASA.

1. No Firepower 2100, o registro da plataforma é ativado por padrão e não pode ser desativado.
2. Não há registro de monitor devido ao fato de que o terminal de monitor não existe nas plataformas FP2100.

Overview Interfaces Logical Devices **Platform Settings**

NTP
SSH
SNMP
HTTPS
DHCP
Syslog
DNS
FIPS and Common Criteria
Access List

Local Destinations Remote Destinations Local Sources

Console

Admin State: Enable
Level: Emergencies Alerts Critical

Platform

Level: Information

File

Admin State: Enable
Level: Critical
Name: messages
Size: 4194304

Save Cancel

As seções **Destinos remotos** e **Origens locais** são idênticas às outras plataformas.

O arquivo de log e os registros ao vivo da plataforma não estão acessíveis através dos comandos CLI.

Dispositivo lógico FTD em FPR2100

No FPR2100, onde o dispositivo FTD está instalado, há duas diferenças principais em comparação com as outras topologias:

1. O endereço IP de origem é o mesmo usado para as mensagens Syslog do dispositivo lógico.
2. Todas as mensagens FXOS são usadas para ID de Syslog e a mensagem para processos genéricos do 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
```

Neste exemplo, há as mensagens Syslog de desligamento da interface.

FAQ

Qual é a porta padrão usada pelo Syslog?

Por padrão, o Syslog usa a porta UDP 514

Você pode configurar o Syslog via TCP?

O syslog via TCP é compatível somente com dispositivos FPR2100 com FTD, em que os Syslogs FXOS são integrados às mensagens do ASA

Informações Relacionadas

- [Guia de configuração da CLI do FXOS](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)