

Firepower可扩展操作系统(FXOS)2.2:使用TACACS+的ISE进行远程管理的机箱身份验证/授权

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[配置](#)

[配置FXOS机箱](#)

[配置ISE服务器](#)

[验证](#)

[FXOS机箱验证](#)

[ISE 2.0验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何通过身份服务引擎(ISE)为Firepower可扩展操作系统(FXOS)机箱配置TACACS+身份验证和授权。

FXOS机箱包括以下用户角色：

- 管理员 — 完成对整个系统的读写访问。默认管理员帐户默认分配此角色，且无法更改。
- 只读 — 对系统配置的只读访问，无权修改系统状态。
- 操作 — 对NTP配置、智能许可的Smart Call Home配置和系统日志（包括系统日志服务器和故障）的读写访问。读取系统其余部分的访问权限。
- AAA — 对用户、角色和AAA配置的读写访问。读取系统其余部分的访问权限。

通过CLI，可以看到如下内容：

```
fpr4120-TAC-A /security* # show role
```

角色：

角色名称 优先级

—

aaa

管理员

运营

只读只读只读

作者：Tony Ramirez、Jose Soto，Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower可扩展操作系统(FXOS)知识
- ISE配置知识
- ISE中需要TACACS+设备管理许可证

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科Firepower 4120安全设备版本2.2
- 虚拟思科身份服务引擎2.2.0.470

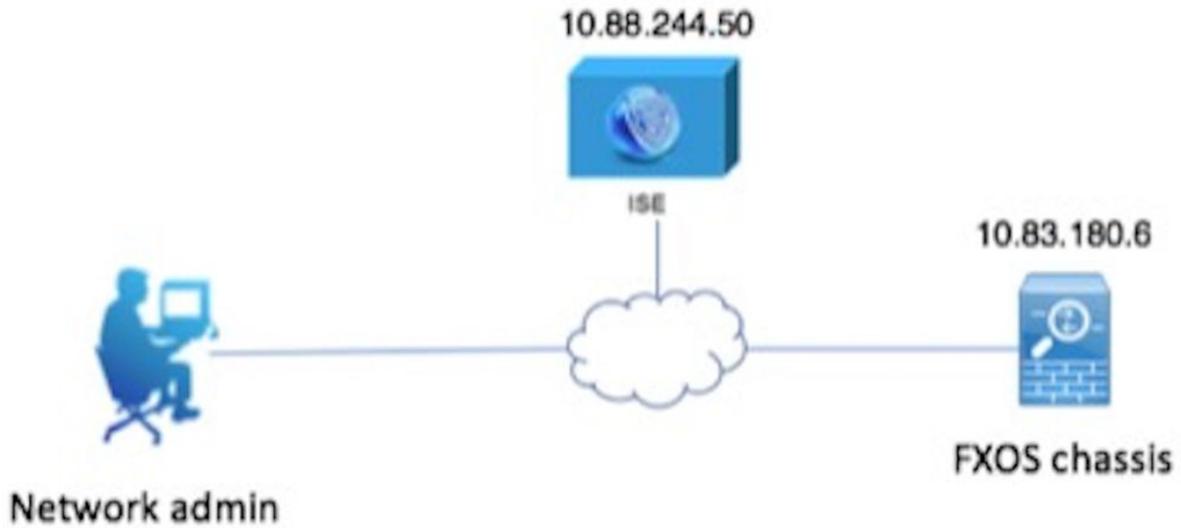
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

配置的目标是：

- 通过ISE对登录FXOS基于Web的GUI和SSH的用户进行身份验证
- 通过ISE根据用户角色授权用户登录FXOS基于Web的GUI和SSH。
- 通过ISE验证FXOS上身份验证和授权的正确操作

网络图



配置

配置FXOS机箱

创建TACACS+提供程序

步骤1. 导航至Platform Settings > AAA。

步骤2. 单击TACACS选项卡。

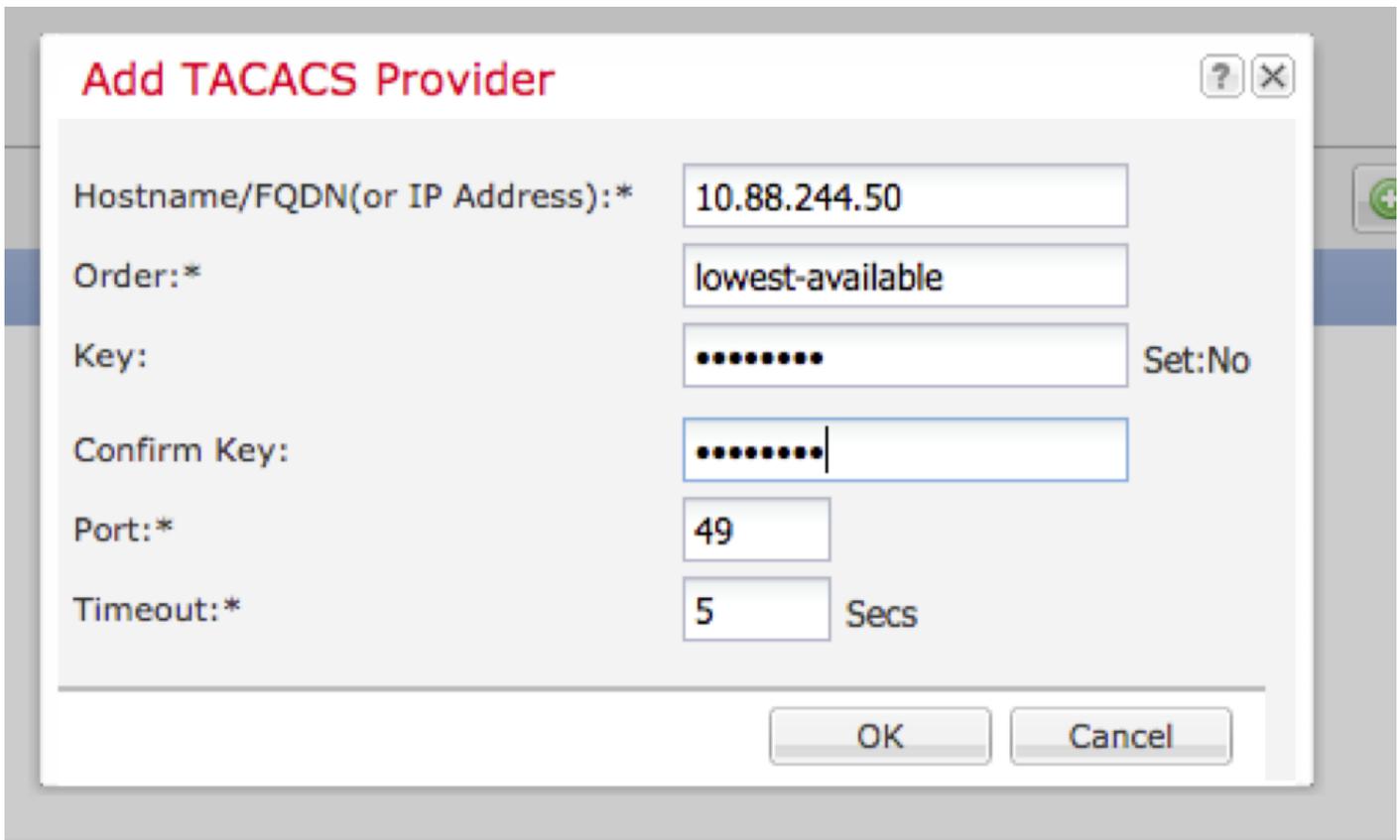


步骤3. 对于要添加的每个TACACS+提供程序（最多16个提供程序）。

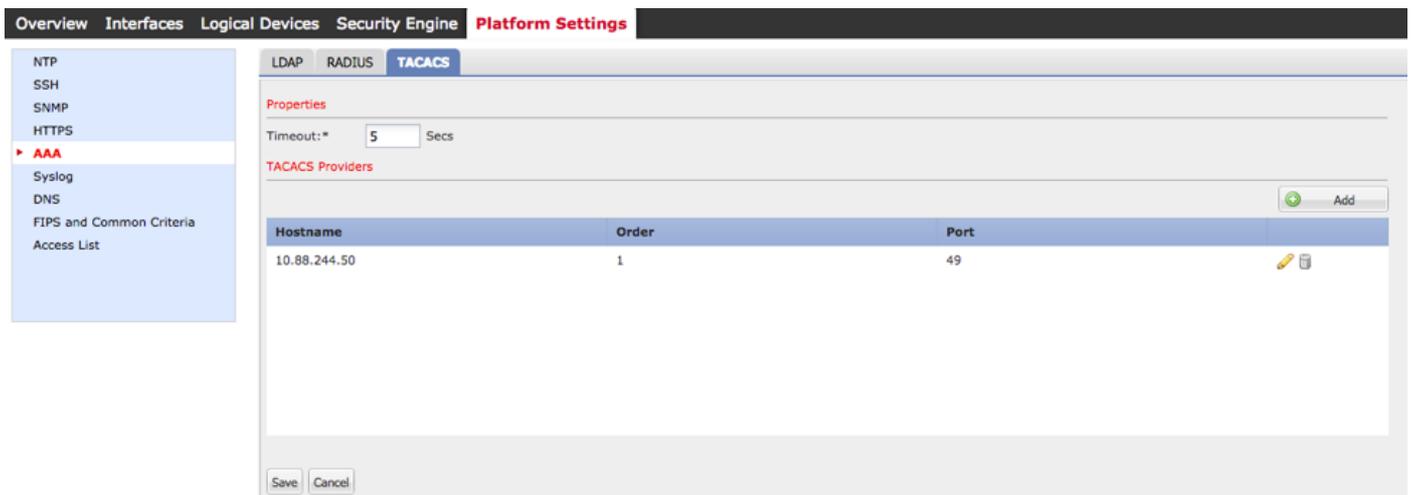
3.1. 在TACACS提供程序区域中，单击**添加**。

3.2. 打开“添加TACACS提供程序”对话框后，输入所需的值。

3.3. 单击“确定”关闭“添加TACACS提供程序”对话框。

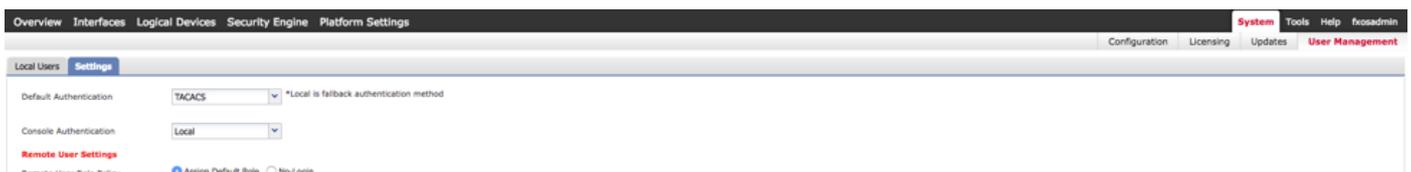


步骤4.单击“保存”。



步骤5.导航至System > User Management > Settings。

步骤6.在Default Authentication下，选择TACACS。



使用CLI创建TACACS+提供程序

步骤1.要启用TACACS身份验证，请运行以下命令。

fpr4120-TAC-A#范围安全

```
fpr4120-TAC-A /security # scope default-auth
```

```
fpr4120-TAC-A /security/default-auth # set realm tacacs
```

步骤2.使用**show detail**命令验证配置。

```
fpr4120-TAC-A /security/default-auth # show detail
```

默认身份验证：

管理领域：塔卡奇

运营领域：塔卡奇

Web会话刷新期（秒）：600

Web、ssh、telnet会话的会话超时（秒）：600

Web、ssh、telnet会话的绝对会话超时（秒）：3600

串行控制台会话超时（秒）：600

串行控制台绝对会话超时（秒）：3600

管理员身份验证服务器组：

操作身份验证服务器组：

第2因素的使用：无

步骤3.要配置TACACS服务器参数，请运行以下命令。

```
fpr4120-TAC-A#范围安全
```

```
fpr4120-TAC-A /security # scope tacacs
```

```
fpr4120-TAC-A /security/tacacs #输入server 10.88.244.50
```

```
fpr4120-TAC-A /security/tacacs/server # set descr "ACS Server"
```

```
fpr4120-TAC-A /security/tacacs/server* # set key
```

输入密钥：*****

确认密钥：*****

步骤4.使用**show detail**命令检验配置。

```
fpr4120-TAC-A /security/tacacs/server* # show detail
```

TACACS+ 服务器:

主机名、FQDN或IP地址：10.88.244.50

描述：

订单：1

端口：49

密钥:****

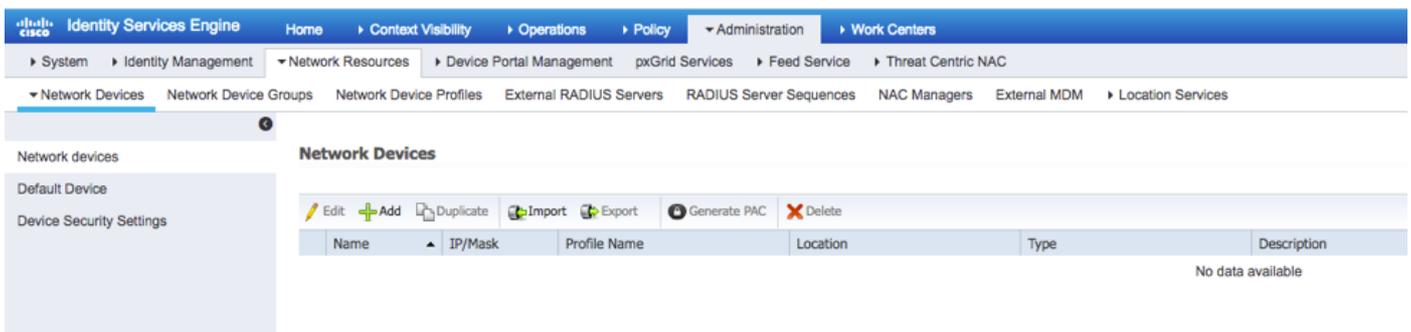
超时：5

配置ISE服务器

将FXOS添加为网络资源

步骤1.导航至Administration > Network Resources > Network Devices。

步骤2.单击ADD。



步骤3.输入所需的值 (Name、IP Address、Device Type和Enable TACACS+并添加KEY) ，单击Submit。

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network devices

Default Device

Device Security Settings

Network Devices List > FXOS

Network Devices

* Name

Description

* IP Address: /

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

IPSEC

Location

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret

Enable Single Connect Mode

Legacy Cisco Device
 TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

创建身份组和用户

步骤1. 导航至 Administration > Identity Management > Groups > User Identity Groups。

步骤2. 单击ADD。

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

Endpoint Identity Groups

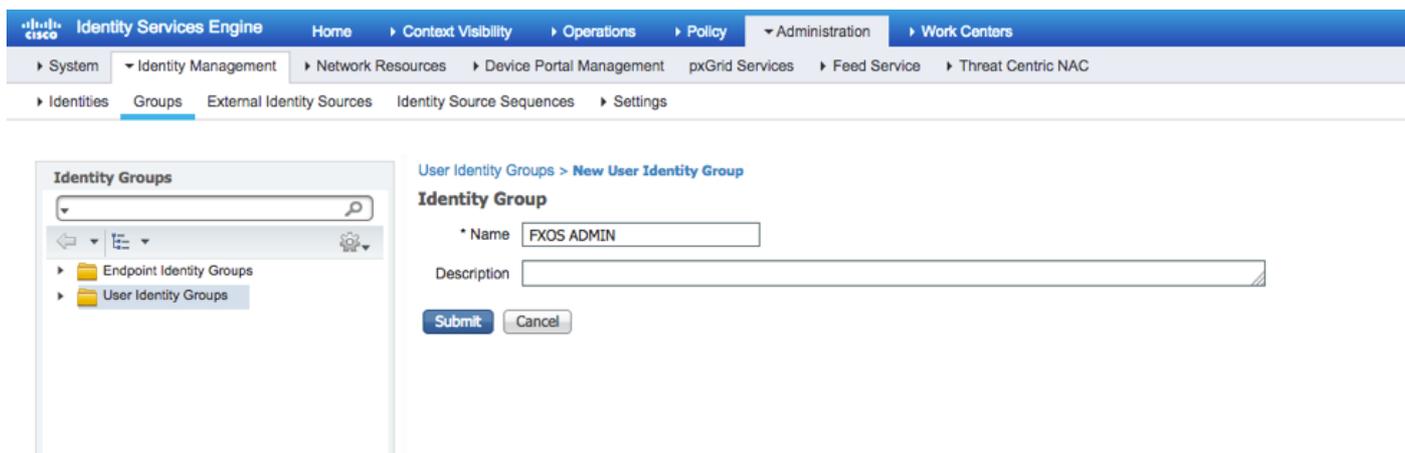
User Identity Groups

User Identity Groups

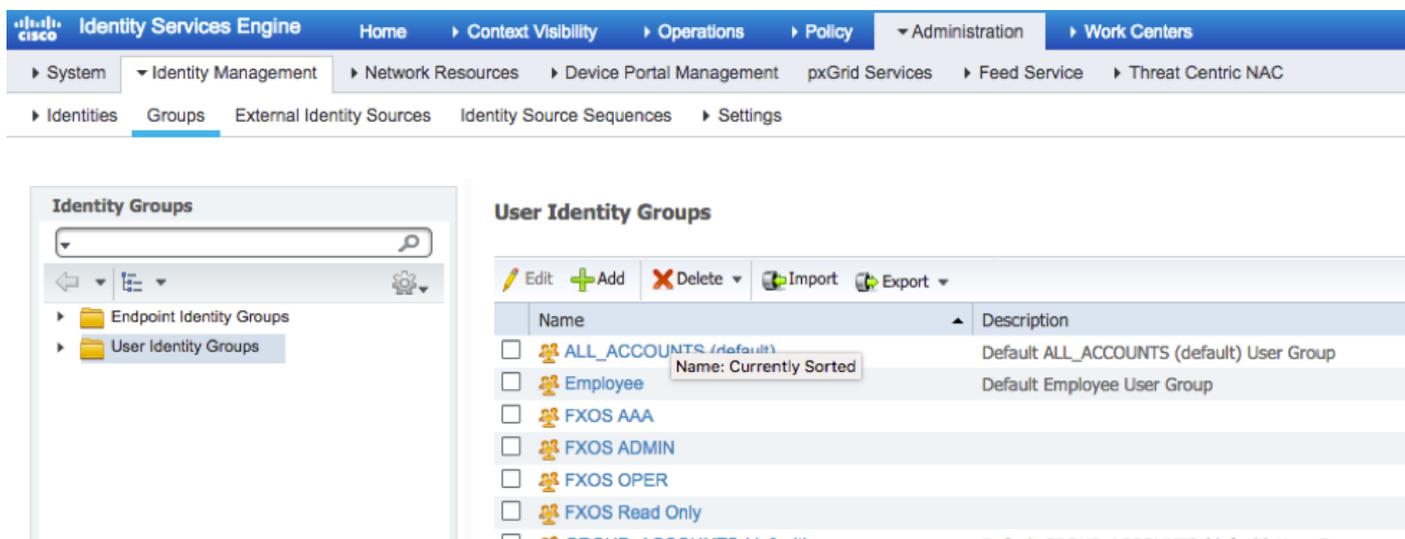
Edit Add Delete Import Export

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/> OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

步骤3.输入名称值，然后单击“提交”。

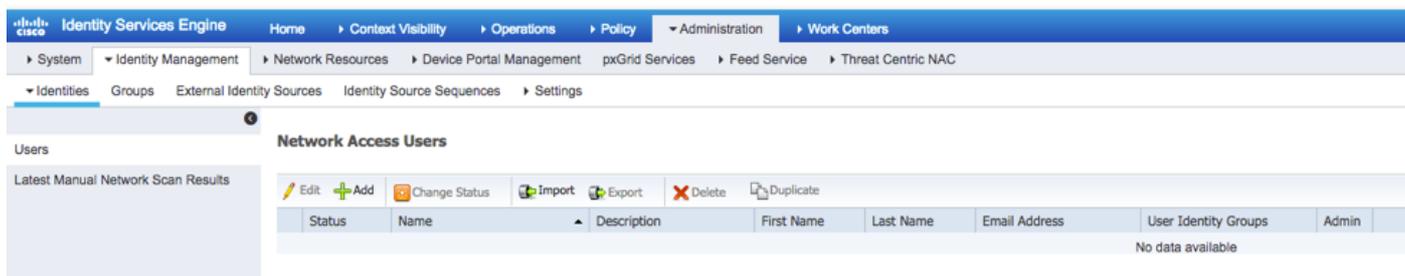


步骤4.对所有所需的用户角色重复步骤3。



步骤5.导航至Administration > Identity Management > Identity > Users。

步骤6.单击ADD。



步骤7.输入所需的值(Name、User Group、Password)。

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

Network Access User

Name:

Status: Enabled

Email:

Passwords

Password Type:

Password: Re-Enter Password:

Enable Password:

User Information

First Name:

Last Name:

Account Options

Description:

Change password on next login:

Account Disable Policy

Disable account if date exceeds (yyyy-mm-dd)

User Groups

步骤8.对所有必需用户重复步骤6。

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users

Edit Add Change Status Import Export Delete Duplicate

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/> Enabled	fxosaaa					FXOS AAA	
<input type="checkbox"/> Enabled	fxosadmin					FXOS ADMIN	
<input type="checkbox"/> Enabled	fxosoper					FXOS OPER	
<input type="checkbox"/> Enabled	fxosro					FXOS Read Only	

为每个用户角色创建外壳配置文件

步骤1.导航至工作中心(Work Centers)>设备管理(Device Administration)>策略元素(Policy Elements)>结果(Results)> TACACS配置文件(TACACS Profiles),然后单击+添加(ADD)。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

TACACS Profiles

0 Selected Rows/Page 4 / 1 / 1 Go 4 Total Rows

Refresh Add Duplicate Trash Edit Filter

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile

步骤2. 输入TACACS配置文件所需的值

2.1. 输入名称。

TACACS Profiles > New

TACACS Profile

Name

Description

Task Attribute View

Raw View

2.2. 在“原始视图”选项卡中，配置以下CISCO-AV-PAIR。

cisco-av-pair=shell:roles="admin"

TACACS Profile

Name

Description

Task Attribute View

Raw View

Profile Attributes

```
cisco-av-pair=shell:roles="admin"
```

Cancel

Submit

2.3.单击“提交”。

TACACS Profile

Name

Description

Task Attribute View Raw View

Common Tasks

Common Task Type

<input type="checkbox"/> Default Privilege	<input type="text"/>	(Select 0 to 15)
<input type="checkbox"/> Maximum Privilege	<input type="text"/>	(Select 0 to 15)
<input type="checkbox"/> Access Control List	<input type="text"/>	
<input type="checkbox"/> Auto Command	<input type="text"/>	
<input type="checkbox"/> No Escape	<input type="text"/>	(Select true or false)
<input type="checkbox"/> Timeout	<input type="text"/>	Minutes (0-9999)
<input type="checkbox"/> Idle Time	<input type="text"/>	Minutes (0-9999)

Custom Attributes

+ Add Trash Edit

Type	Name	Value	
<input type="checkbox"/> MANDATORY	cisco-av-pair	shell:roles="admin"	

Cancel Save

步骤3.使用以下Cisco-AV-Pair对剩余的用户角色重复步骤2。

`cisco-av-pair=shell:roles="aaa"`

`cisco-av-pair=shell:roles="operations"`

`cisco-av-pair=shell:roles="只读"`

Custom Attributes

+ Add Trash Edit

Type	Name	Value	
<input type="checkbox"/> MANDATORY	cisco-av-pair	shell:roles="aaa"	

Cancel Save

Custom Attributes

<input type="checkbox"/>	Type	Name	Value	
<input type="checkbox"/>	MANDATORY	cisco-av-pair	shell:roles="operations"	 

Custom Attributes

<input type="checkbox"/>	Type	Name	Value	
<input type="checkbox"/>	MANDATORY	cisco-av-pair	shell:roles="read-only"	 

TACACS Profiles

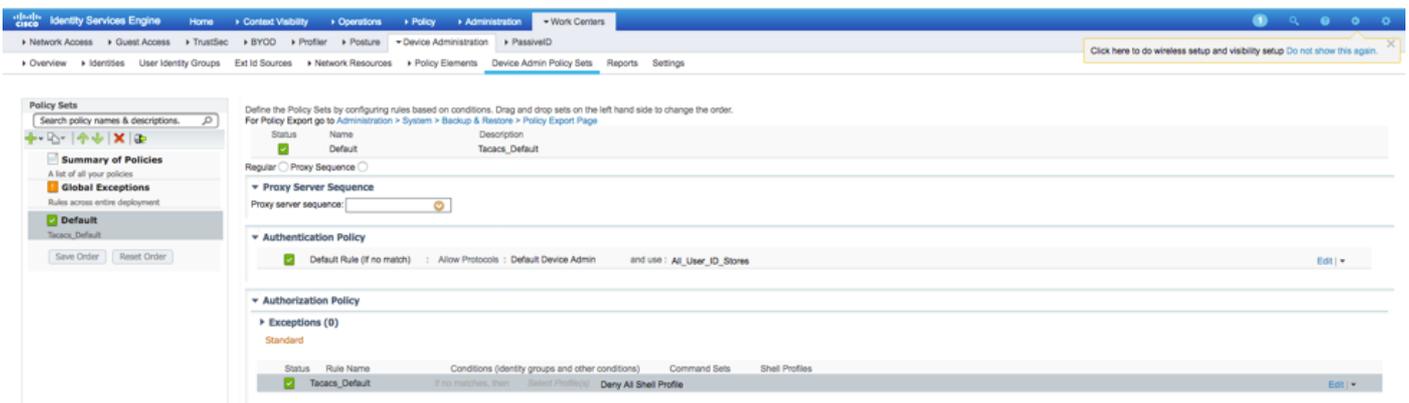
0 Selected

Rows/Page 1 / 1 8 Total Rows

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	FXOS_Admin_Profile	Shell	
<input type="checkbox"/>	FXOS_AAA_Shell	Shell	
<input type="checkbox"/>	FXOS_Operations_Shell	Shell	
<input type="checkbox"/>	FXOS_ReadOnly_Shell	Shell	

创建TACACS授权策略

步骤1. 导航至 Work Centers > Device Administration > Device Admin Policy Sets.



The screenshot displays the Cisco ISE configuration interface for Device Admin Policy Sets. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Device Admin Policy Sets. The main content area shows the configuration for the 'Tacacs_Default' policy set. The 'Default Rule (if no match)' is set to 'Allow Protocols : Default Device Admin and use : All_User_ID_Stores'. Under the 'Authorization Policy' section, there is an 'Exceptions (0)' list with one exception: 'Deny All Shell Profile'.

步骤2. 确保身份验证策略指向内部用户数据库或所需的身份库。



步骤3. 点击默认授权策略末尾的箭头，然后点击上方的插入规则。

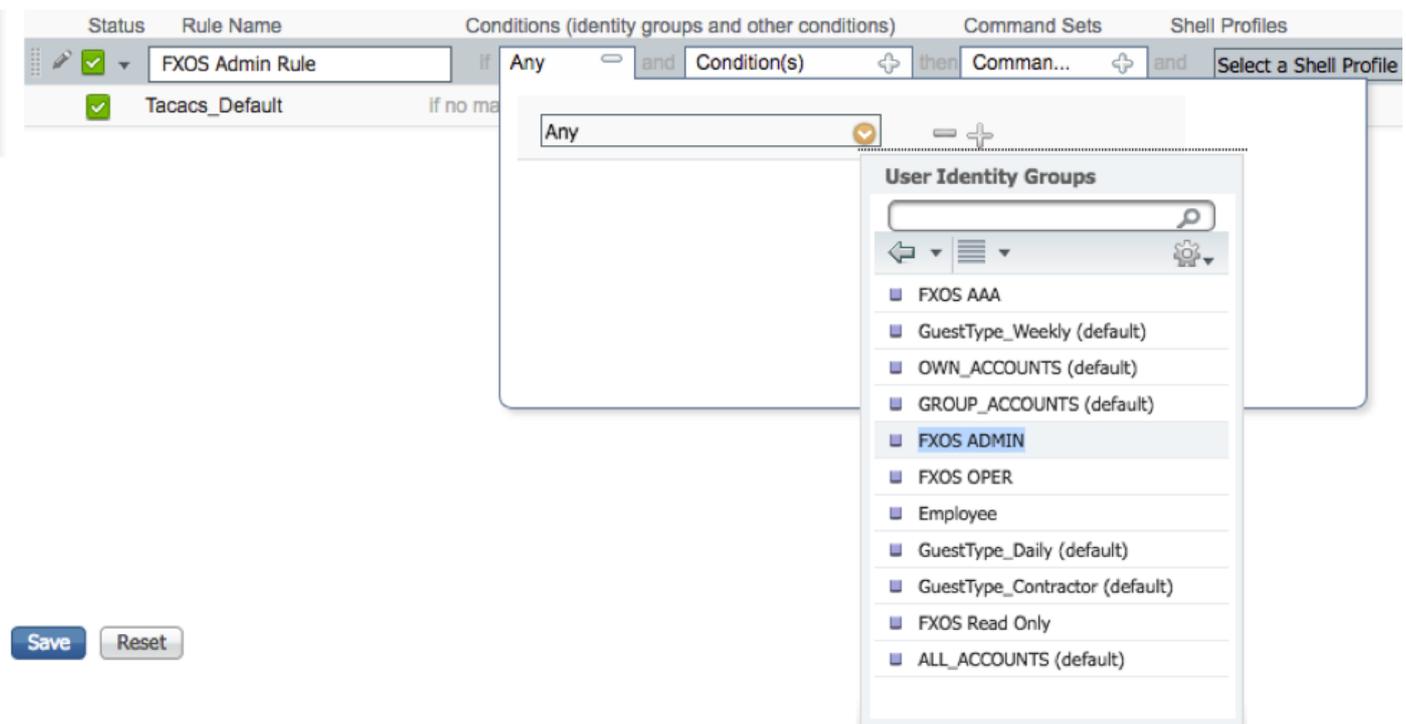


步骤4. 输入具有所需参数的规则值：

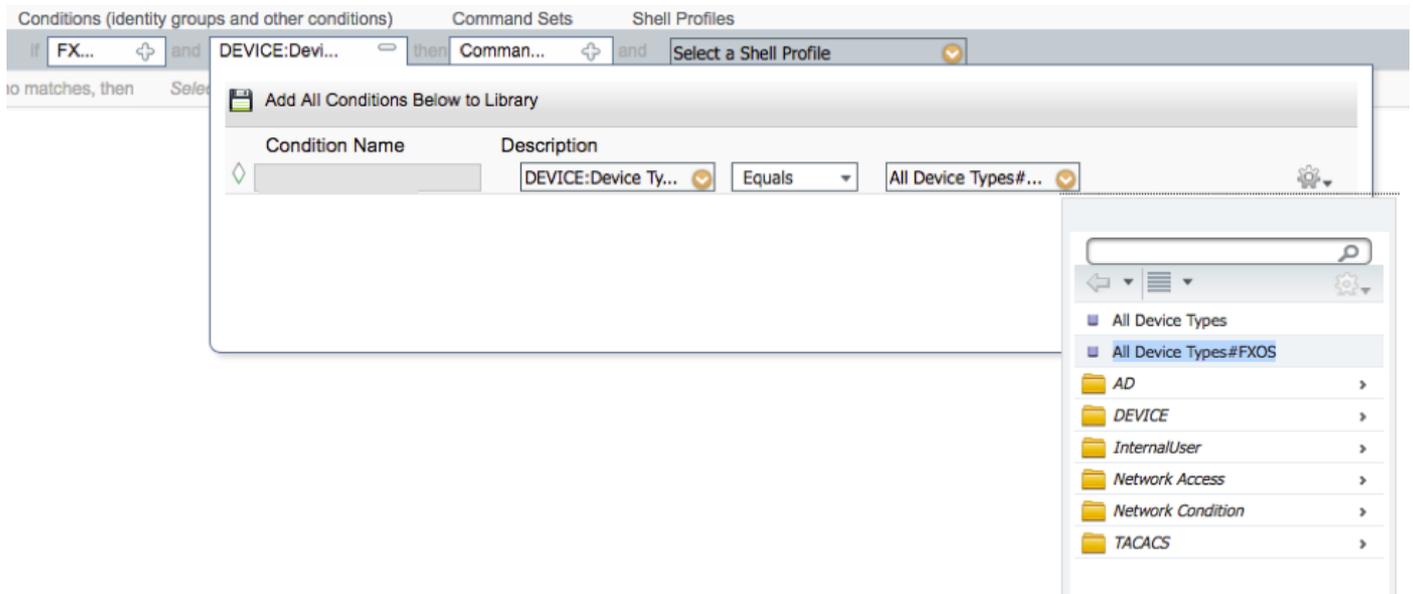
4.1. 规则名称：FXOS管理规则。

4.2. 条件。

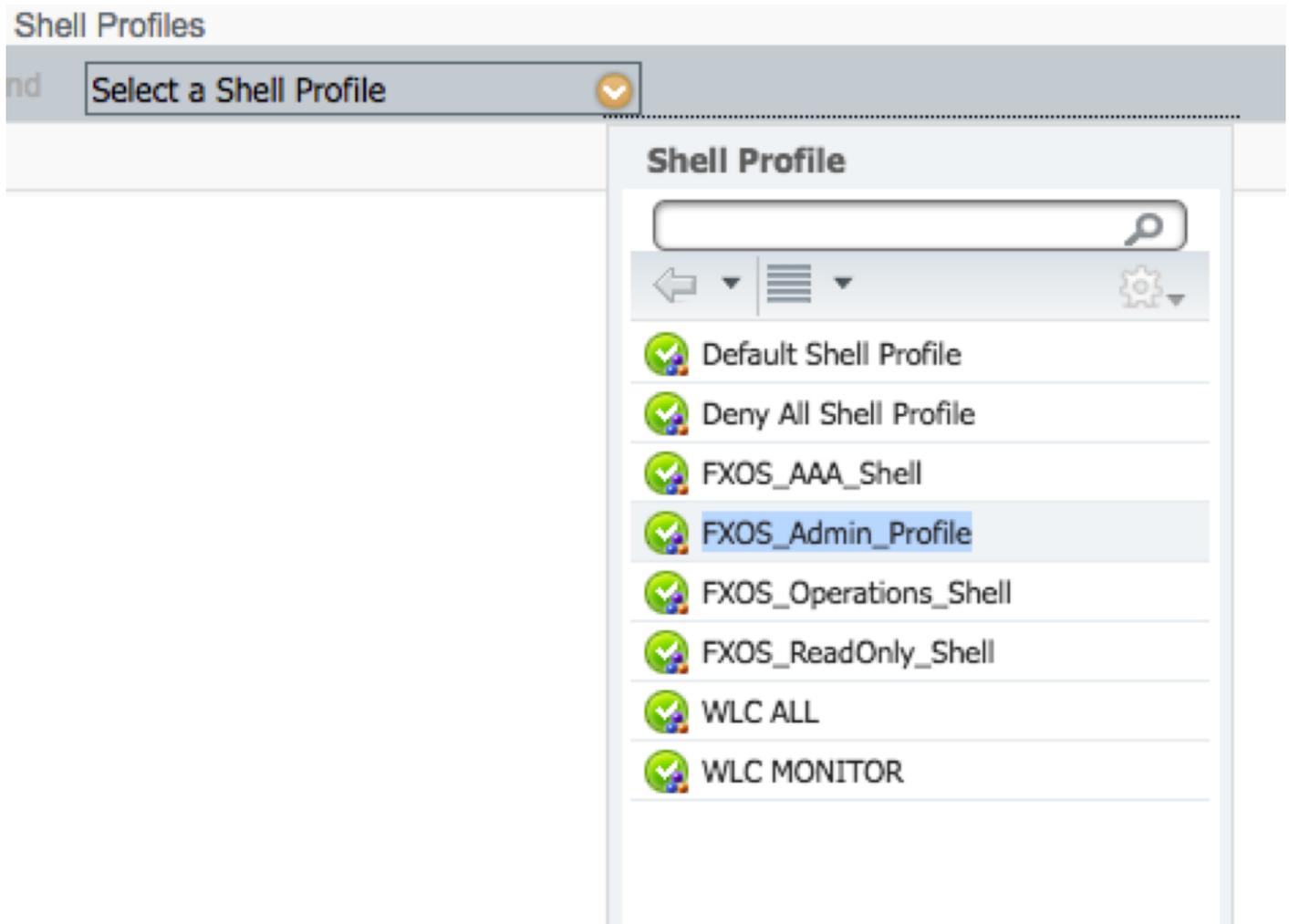
如果：用户身份组为FXOS ADMIN



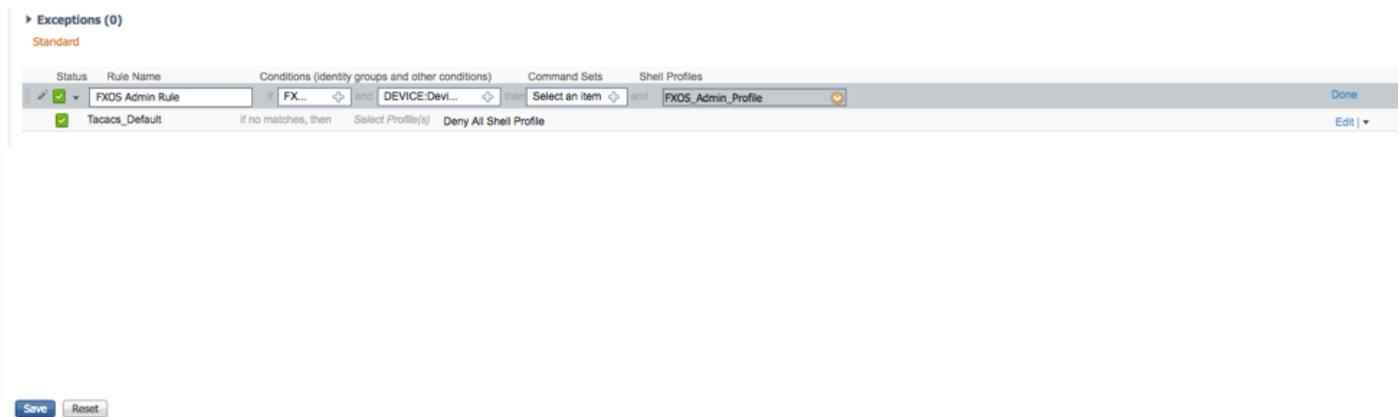
设备：设备类型等于所有设备类型#FXOS



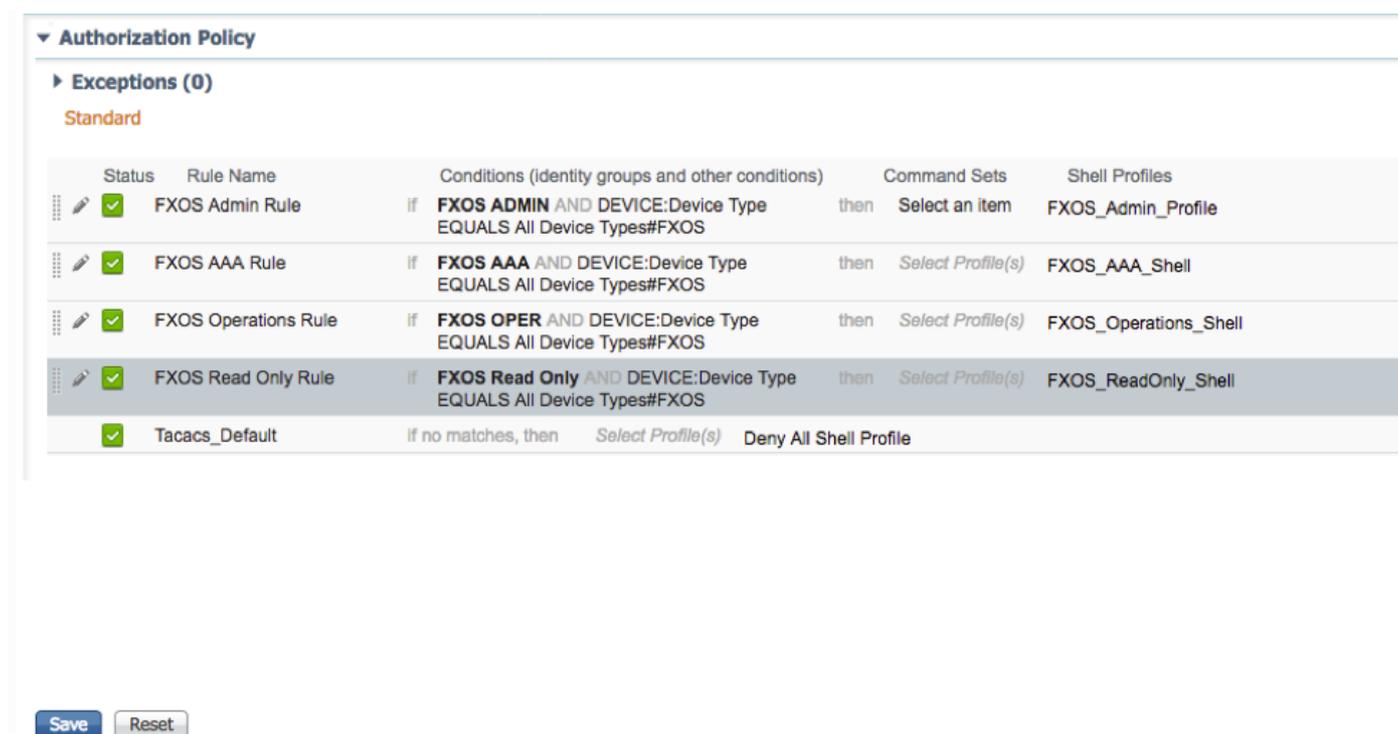
外壳配置文件：FXOS_Admin_Profile



步骤5.单击“完成”。



步骤6.对其余用户角色重复步骤3和4，完成后单击**SAVE**。



验证

您现在可以测试每个用户并验证分配的用户角色。

FXOS机箱验证

1. Telnet或SSH至FXOS机箱，并使用ISE上任何已创建的用户登录。

username : fxosadmin

密码 :

fpr4120-TAC-A#范围安全

fpr4120-TAC-A /security # **show remote-user detail**

远程用户fxosaa:

描述:

用户角色:

名称 : **aaa**

名称 : **只读**

远程用户**fxosadmin**:

描述:

用户角色:

名称 : **admin**

名称 : **只读**

远程用户**fxosoper**:

描述:

用户角色:

名称 : **运营**

名称 : **只读**

远程用户**fxosro**:

描述:

用户角色:

名称 : **只读**

根据输入的用户名 , FXOS机箱cli将仅显示为分配的用户角色授权的命令。

管理员用户角色。

fpr4120-TAC-A /security #?

确认确认

clear-user-sessionsclear User Sessions

创建托管对象

删除托管对象

禁用禁用服务

启用服务

输入管理对象

范围更改当前模式

设置属性值

显示系统信息

终止活动CIMC会话

```
fpr4120-TAC-A#connect fxos
```

```
fpr4120-TAC-A(fxos)# debug aaa aaa-requests
```

```
fpr4120-TAC-A(fxos)#
```

只读用户角色。

```
fpr4120-TAC-A /security #?
```

范围更改当前模式

设置属性值

显示系统信息

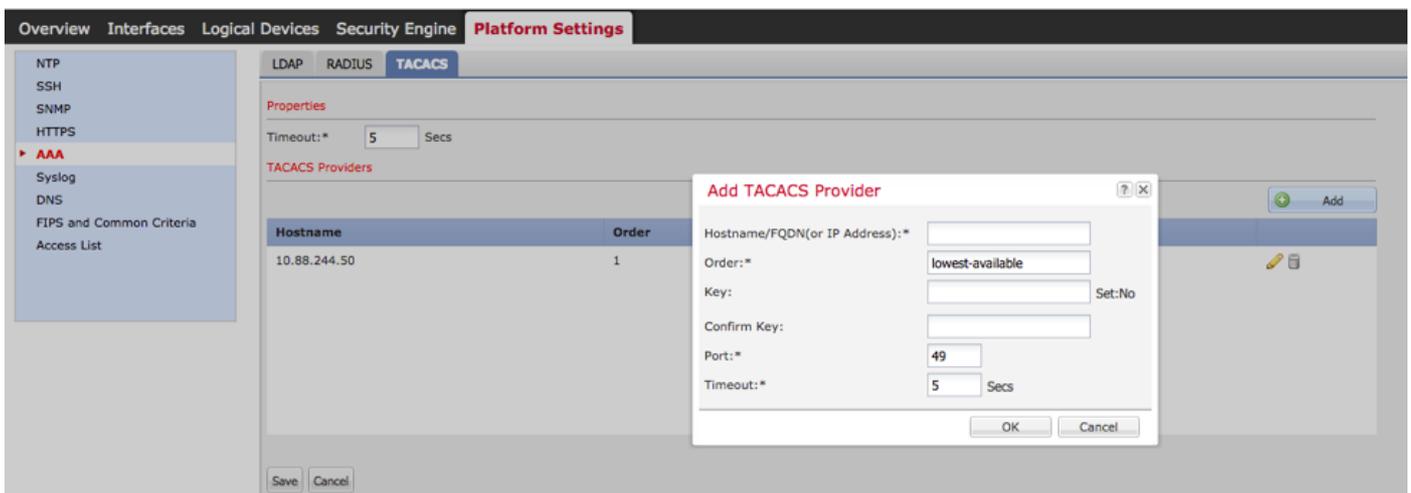
```
fpr4120-TAC-A#connect fxos
```

```
fpr4120-TAC-A(fxos)# debug aaa aaa-requests
```

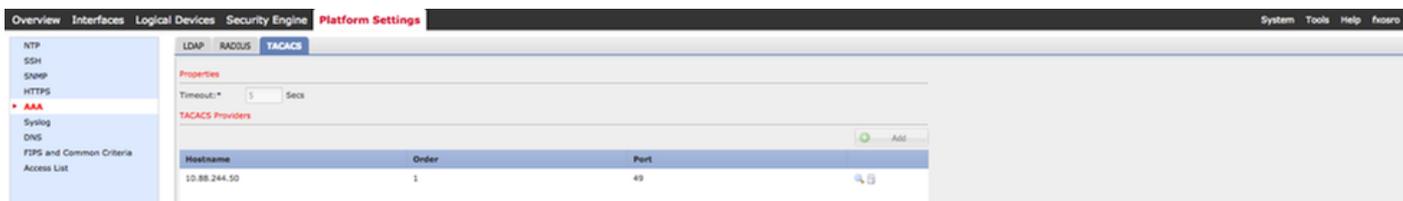
拒绝角色的权限百分比

2.浏览到FXOS机箱IP地址，然后使用ISE上任何已创建的用户登录。

管理员用户角色。



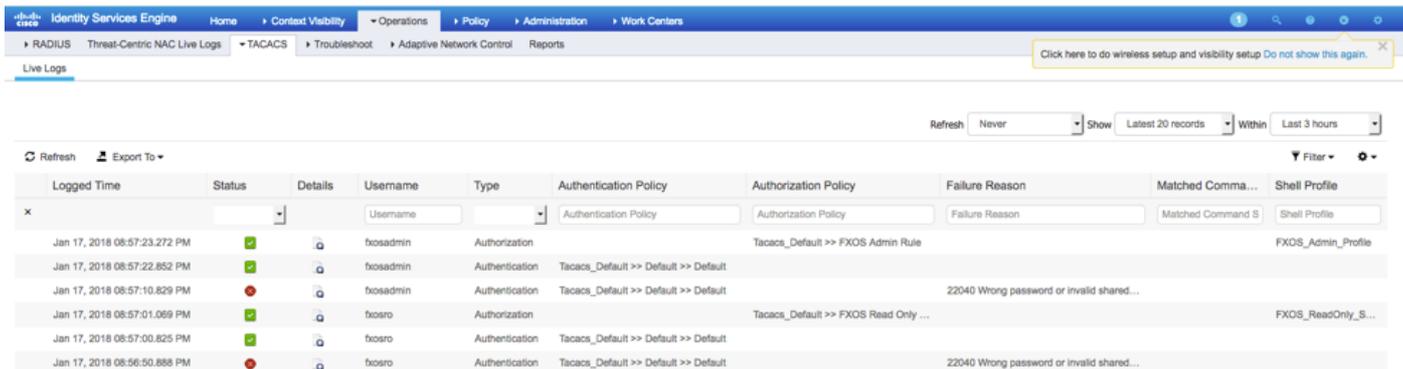
只读用户角色。



注意：请注意，“添加”按钮呈灰色显示。

ISE 2.0

1.“>”“TACACS”



故障排除

要调试AAA身份验证和授权，请在FXOS cli中运行以下命令。

```
fr4120-TAC-A#connect fxos
```

```
fr4120-TAC-A(fxos)# debug aaa aaa-requests
```

```
fr4120-TAC-A(fxos)# debug aaa event
```

```
fr4120-TAC-A(fxos)# debug aaa errors
```

```
fr4120-TAC-A(fxos)#期限监控器
```

身份验证尝试成功后，您将看到以下输出。

```
2018年1月17日 15:46:40.305247 aaa:aaa_req_process进行身份验证。session no 0
```

```
2018年1月17日 15:46:40.305262 aaa:aaa_req_process:来自应用的常规AAA请求：login  
appln_subtype:默认
```

```
2018年1月17日 15:46:40.305271 aaa:try_next_aaa_method
```

```
2018年1月17日 15:46:40.305285 aaa:配置的方法总数为1，当前要尝试的索引为0
```

```
2018年1月17日 15:46:40.305294 aaa:handle_req_using_method
```

```
2018年1月17日 15:46:40.305301 aaa:AAA_METHOD_SERVER_GROUP
```

2018年1月17日15:46:40.305308 aaa:aaa_sg_method_handler group = tacacs

2018年1月17日15:46:40.305315 aaa:使用传递给此函数的sg_protocol

2018年1月17日15:46:40.305324 aaa:正在向TACACS服务发送请求

2018年1月17日15:46:40.305384 aaa:已成功配置方法组

2018年1月17日15:46:40.554631 aaa:aaa_process_fd_set

2018年1月17日15:46:40.555229 aaa:aaa_process_fd_set:aaa_q上的mtscallback

2018年1月17日15:46:40.555817 aaa:mts_message_response_handler:MTS响应

2018年1月17日15:46:40.556387 aaa:prot_daemon_reponse_handler

2018年1月17日15:46:40.557042 aaa:会话 : 0x8dfd68c已从会话表0中删除

2018年1月17日15:46:40.557059 aaa:is_aaa_resp_status_success状态= 1

2018年1月17日15:46:40.557066 aaa:is_aaa_resp_status_success为TRUE

2018年1月17日15:46:40.557075 aaa:aaa_send_client_response以进行身份验证。session->flags=21。aaa_resp->flags=0。

2018年1月17日15:46:40.557083 aaa:AAA_REQ_FLAG_NORMAL

2018年1月17日15:46:40.557106 aaa:mts_send_response成功

2018年1月17日15:46:40.557364 aaa:aaa_req_process进行授权。session no 0

2018年1月17日15:46:40.557378 aaa:aaa_req_process通过来自应用的上下文调用 : login appln_subtype:default authen_type:2, authen_method:0

2018年1月17日15:46:40.557386 aaa:aaa_send_req_using_context

2018年1月17日15:46:40.557394 aaa:aaa_sg_method_handler组= (空)

2018年1月17日15:46:40.557401 aaa:使用传递给此函数的sg_protocol

2018年1月17日15:46:40.557408 aaa:基于情景或定向AAA请求(例外 : 不是中继请求)。不会复制AAA请求

2018年1月17日15:46:40.557415 aaa:正在向TACACS服务发送请求

2018年1月17日15:46:40.801732 aaa:aaa_send_client_response以进行授权。session->flags=9。aaa_resp->flags=0。

2018年1月17日15:46:40.801740 aaa:AAA_REQ_FLAG_NORMAL

2018年1月17日15:46:40.801761 aaa:mts_send_response成功

2018年1月17日15:46:40.848932 aaa:旧操作码 : accounting_interim_update

2018年1月17日15:46:40.848943 aaa:aaa_create_local_acct_req:user=, session_id=, log=added user:fxosadmin to role:admin

2018年1月17日15:46:40.848963 aaa:aaa_req_process , 用于记帐。 session no 0

2018年1月17日15:46:40.848972 aaa:MTS请求引用为NULL。本地请求

2018年1月17日15:46:40.848982 aaa:设置AAA_REQ_RESPONSE_NOT_NEEDED

2018年1月17日15:46:40.848992 aaa:aaa_req_process:来自应用的常规AAA请求 : default appln_subtype:默认

2018年1月17日15:46:40.849002 aaa:try_next_aaa_method

2018年1月17日15:46:40.849022 aaa:没有默认配置方法

2018年1月17日15:46:40.849032 aaa:此请求没有可用的配置

2018年1月17日15:46:40.849043 aaa:try_fallback_method

2018年1月17日15:46:40.849053 aaa:handle_req_using_method

2018年1月17日15:46:40.849063 aaa:local_method_handler

2018年1月17日15:46:40.849073 aaa:aaa_local_accounting_msg

2018年1月17日15:46:40.849085 aaa:更新 : : 已添加用户 : fxosadmin到角色 : admin

身份验证尝试失败后 , 您将看到以下输出。

2018年1月17日15:46:17.836271 aaa:aaa_req_process进行身份验证。 session no 0

2018年1月17日15:46:17.836616 aaa:aaa_req_process:来自应用的常规AAA请求 : login appln_subtype:默认

2018年1月17日15:46:17.837063 aaa:try_next_aaa_method

2018年1月17日15:46:17.837416 aaa:配置的方法总数为1 , 当前要尝试的索引为0

2018年1月17日15:46:17.837766 aaa:handle_req_using_method

2018年1月17日15:46:17.838103 aaa:AAA_METHOD_SERVER_GROUP

2018年1月17日15:46:17.838477 aaa:aaa_sg_method_handler group = tacacs

2018年1月17日15:46:17.838826 aaa:使用传递给此函数的sg_protocol

2018年1月17日15:46:17.839167 aaa:正在向TACACS服务发送请求

2018年1月17日15:46:17.840225 aaa:已成功配置方法组

2018年1月17日15:46:18.043710 aaa:is_aaa_resp_status_success状态= 2

2018年1月17日 15:46:18.044048 aaa:is_aaa_resp_status_success为TRUE

2018年1月17日 15:46:18.044395 aaa:aaa_send_client_response以进行身份验证。session->flags=21。aaa_resp->flags=0。

2018年1月17日 15:46:18.044733 aaa:AAA_REQ_FLAG_NORMAL

2018年1月17日 15:46:18.045096 aaa:mts_send_response成功

2018年1月17日 15:46:18.045677 aaa:aaa_cleanup_session

2018年1月17日 15:46:18.045689 aaa:mts_drop request msg

2018年1月17日 15:46:18.045699 aaa:aaa_req应被释放。

2018年1月17日 15:46:18.045715 aaa:aaa_process_fd_set

2018年1月17日 15:46:18.045722 aaa:aaa_process_fd_set:aaa_q上的mtscallback

2018年1月17日 15:46:18.045732 aaa:aaa_enable_info_config:GET_REQ for aaa login错误消息

2018年1月17日 15:46:18.045738 aaa:返回配置操作的返回值：未知安全项

相关信息

启用TACACS/RADIUS身份验证时，FX-OS CLI上的Ethanalyzer命令将提示输入密码。此行为由Bug引起。

Bug ID: [CSCvg87518](#)