Firepower可扩展操作系统(FXO) 2.2 ：远程管理的机箱认证/授权与ISE使用RADIUS

目录

简介

本文描述如何通过身份服务引擎(ISE)配置RADIUS验证和授权Firepower可扩展操作系统的(FXO)机箱的。

FXO机箱包括以下用户角色：

- 管理员-对整个系统的完整读写访问。默认管理帐户分配此角色默认情况下，并且不可能更改。
- 只读-对系统配置的只读访问没有权限修改系统状态。
- 操作-对NTP配置、聪明的Call Home配置聪明许可授权的和系统日志的读写访问，包括系统日志服务器和故障。对系统的其余的读访问。
- AAA -对用户、角色和AAA配置的读写访问。对系统的其余的读访问。

通过CLI这能被看到如下：

```
fpr4120-TAC-A /security * #请显示角色

角色：

  角色命名Priv

  ----------       ----

  aaa aaa

  admin admin
```

操作操作

只读只读

贡献用托尼雷米雷斯，何塞索托， Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- 知识Firepower可扩展操作系统(FXO)
- ISE配置知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Firepower 4120安全工具版本2.2
- 虚拟思科身份服务引擎2.2.0.470

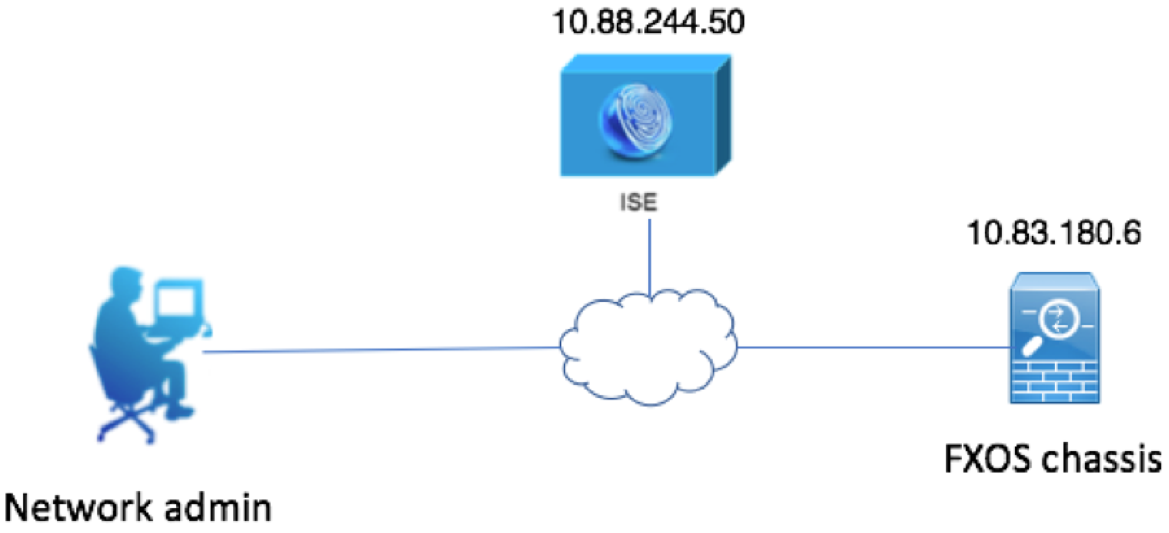
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

配置的目标对：

- 验证登录FXOS的基于Web的GUI和SSH的用户通过ISE
- 认证登录FXOS的基于Web的GUI和SSH的用户根据他们的各自用户角色通过ISE。
- 通过ISE验证认证和授权正常操作在FXO的

网络图



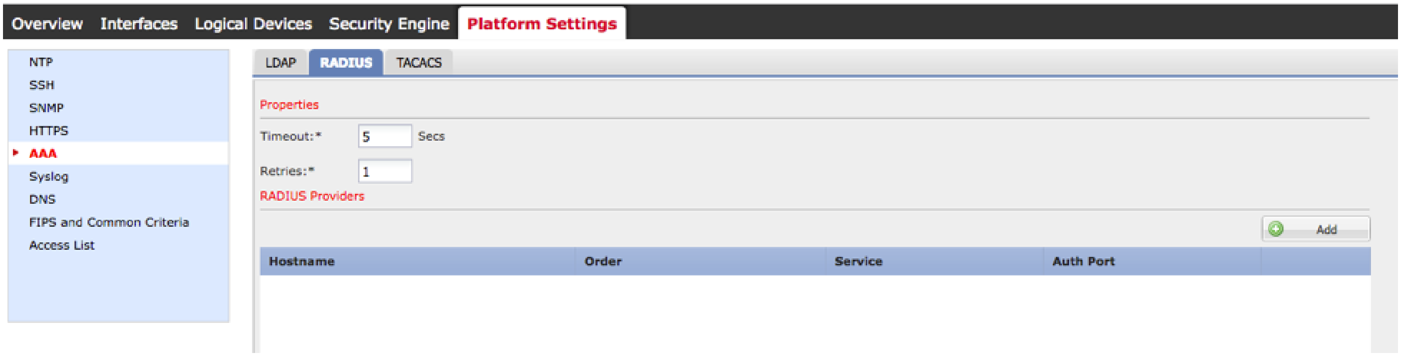
配置

配置FXO机箱

创建使用机箱管理器的RADIUS供应商

步骤1.导航对**平台设置>AAA。**

步骤2.点击**RADIUS选项**。



Properties

Timeout:* 5 Secs

Retries:* 1

RADIUS Providers

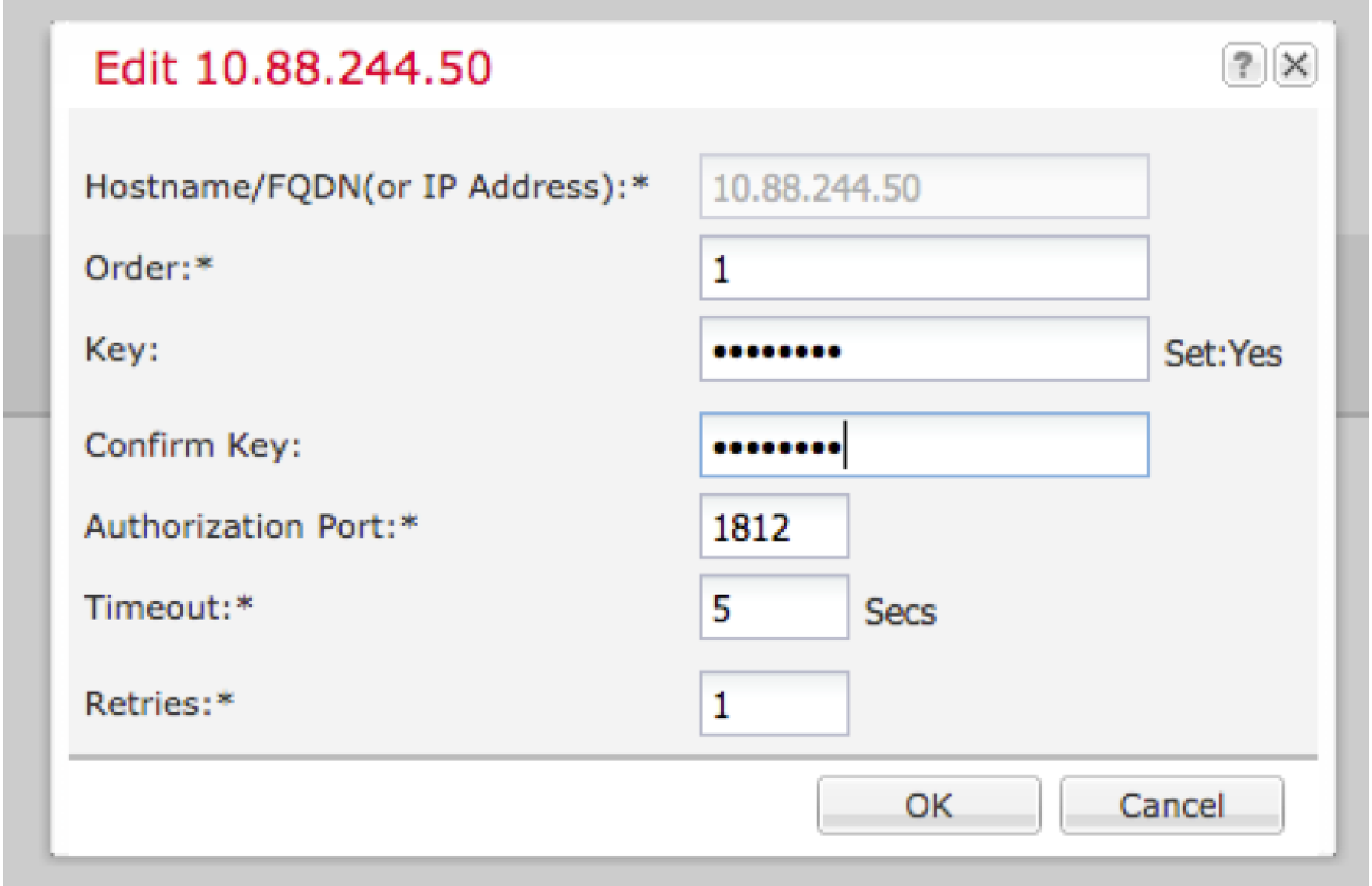
Hostname	Order	Service	Auth Port

第三步：每个RADIUS供应商您想要添加(16个供应商)。

3.1. 在RADIUS供应商地区中，请单击**添加。**

3.2. 一旦添加RADIUS供应商对话框打开，请输入需要的值。

3.3. 点击OK键关闭添加RADIUS供应商对话框。



Edit 10.88.244.50

Hostname/FQDN(or IP Address):* 10.88.244.50

Order:* 1

Key: ●●●●●●●● Set:Yes

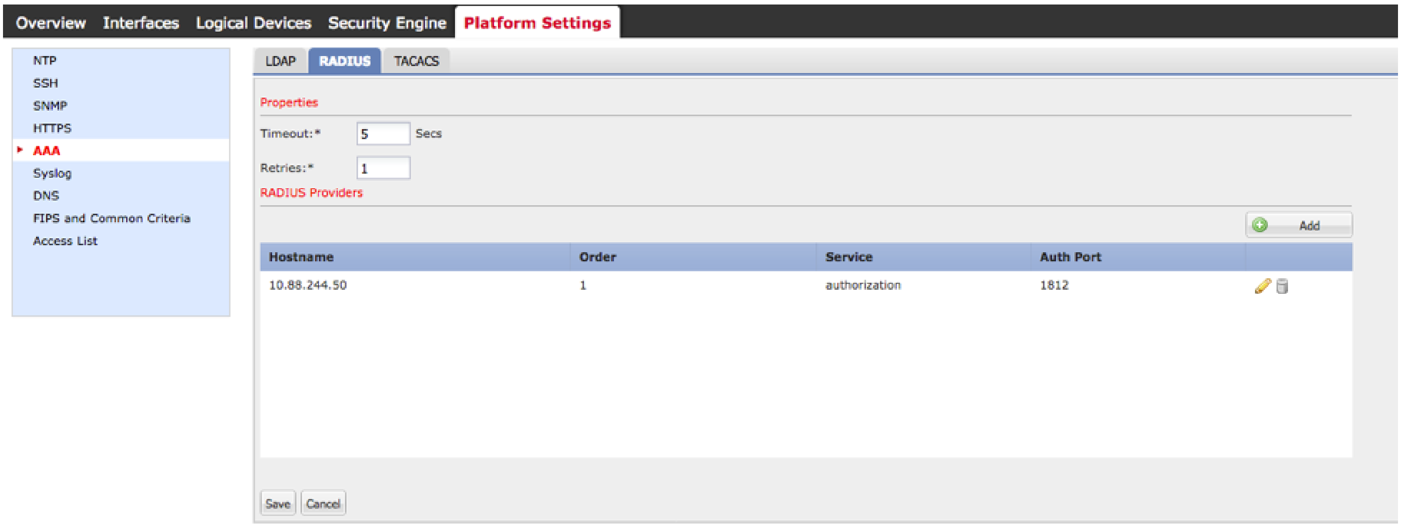
Confirm Key: ●●●●●●●●

Authorization Port:* 1812

Timeout:* 5 Secs

Retries:* 1

步骤4.点击“**Save**”。



Properties

Timeout:* 5 Secs

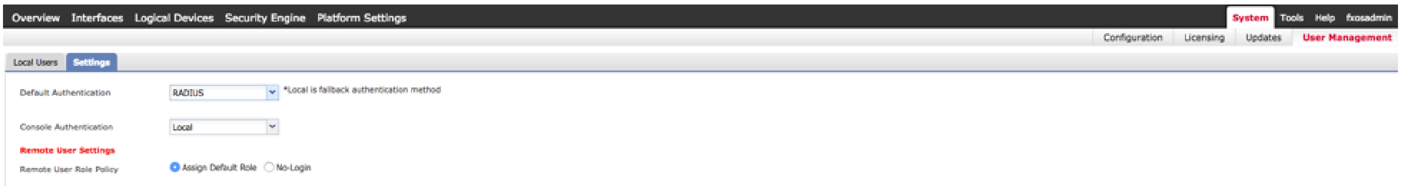
Retries:* 1

RADIUS Providers

Hostname	Order	Service	Auth Port
10.88.244.50	1	authorization	1812

步骤5.导航对**系统>用户管理>设置**。

第六步：在默认验证下请选择**RADIUS**。



Default Authentication RADIUS *Local is fallback authentication method

Console Authentication Local

Remote User Settings

Remote User Role Policy ● Assign Default Role ○ No-Login

创建使用CLI的RADIUS供应商

步骤1.为了启用RADIUS验证，请运行以下命令。

```
fpr4120-TAC-A#范围安全

fpr4120-TAC-A /security #范围默认验证

fpr4120-TAC-A /security/default-auth #集领域radius
```

第二步：请使用**detail命令的显示**显示结果。

```
fpr4120-TAC-A /security/default-auth #显示详细信息

默认验证：

  Admin领域：Radius

  可操作的领域：Radius

  Web会话刷新期限(以秒) ：600

  会话超时(以秒) Web的， SSH，远程登录会话：600

  绝对会话超时(以秒) Web的， SSH，远程登录会话：3600

  串行控制台会话超时(以秒) ：600

  串行控制台绝对会话超时(以秒) ：3600

  Admin认证服务器组：

  可操作的认证服务器组：

  使用第2个要素：无
```

步骤3.为了配置RADIUS服务器参数请运行以下命令。

```
fpr4120-TAC-A#范围安全

fpr4120-TAC-A /security #范围radius

fpr4120-TAC-A /security/radius #回车服务器10.88.244.50

fpr4120-TAC-A /security/radius/server #集descr “ISE服务器”

fpr4120-TAC-A /security/radius/server * #集密钥

输入密钥：******

确认密钥：******
```

第四步：请使用**detail命令的显示**显示结果。

```
fpr4120-TAC-A /security/radius/server * #请显示详细信息
```

RADIUS服务器：

主机名、FQDN或者IP地址：10.88.244.50

Descr ：

命令：1

验证波尔特：1812

密钥：****

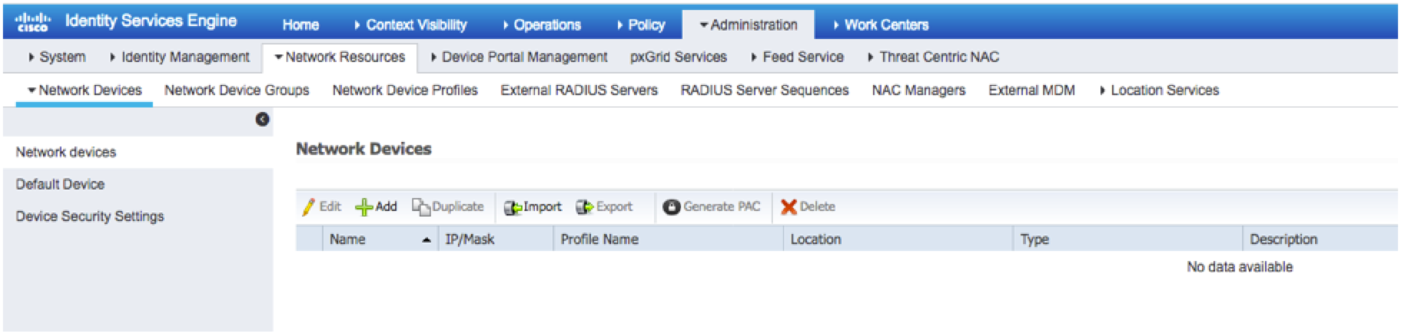
超时：5

配置ISE服务器

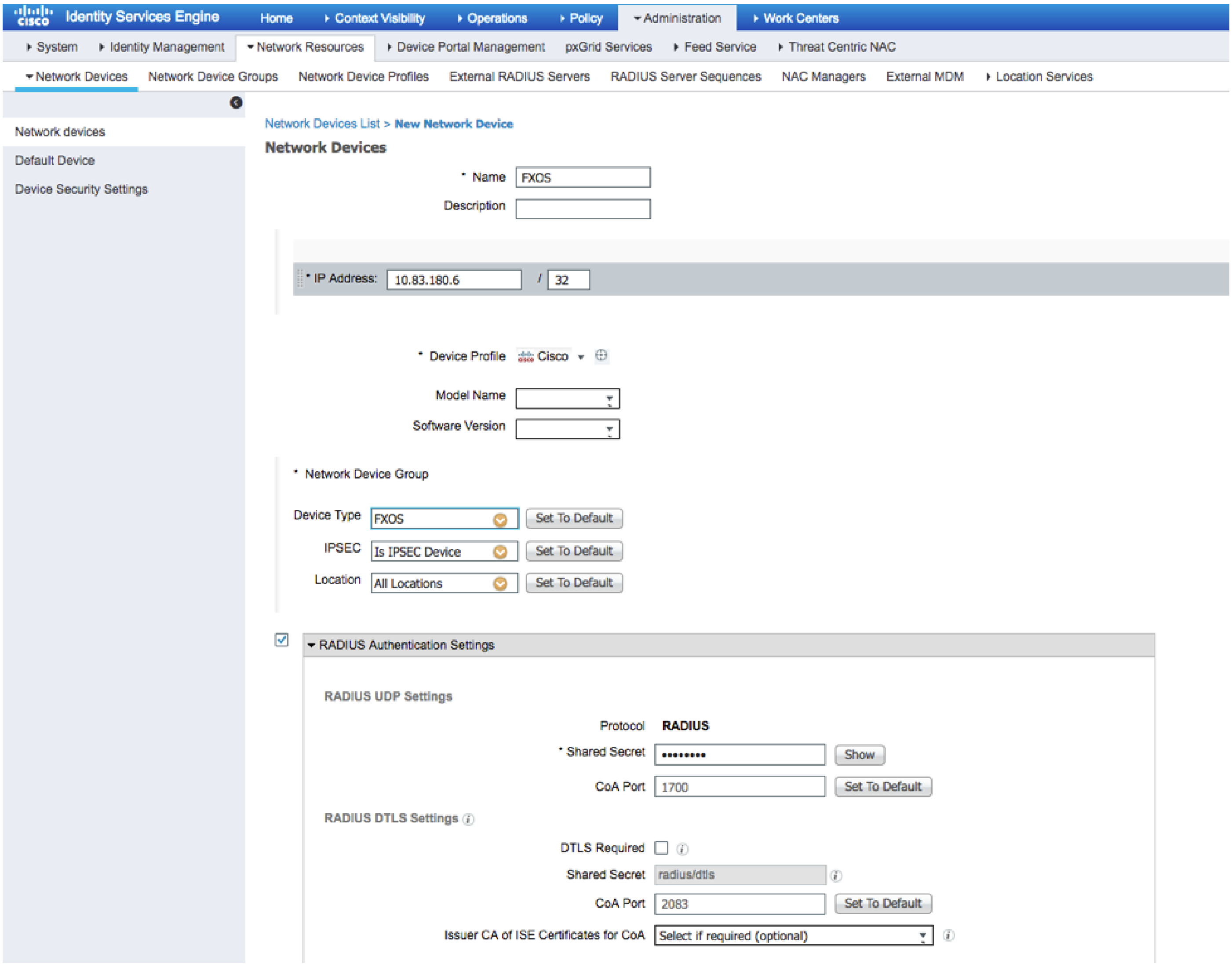
添加FXO作为网络资源

步骤1.导航到**Administration >网络资源>网络设备。**

步骤2.单击**添加**



步骤3.输入需要的值(名称、IP地址、设备类型和Enable (event) RADIUS和添加KEY)，单击**提交。**



Network Devices List > New Network Device

Network Devices

* Name: FXOS

Description:

* IP Address: 10.83.180.6 / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Device Type: FXOS

IPSEC: Is IPSEC Device

Location: All Locations

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

* Shared Secret: ••••••••

CoA Port: 1700

RADIUS DTLS Settings

DTLS Required: □

Shared Secret: radius/dtls

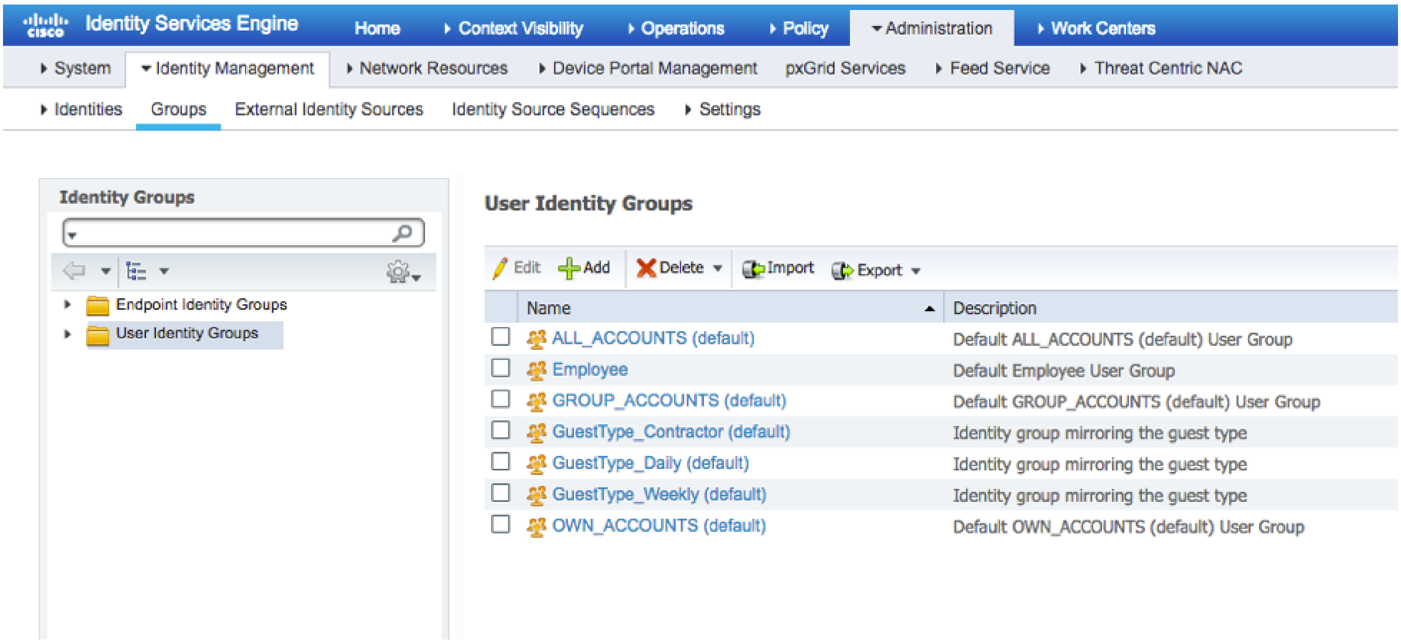
CoA Port: 2083

Issuer CA of ISE Certificates for CoA: Select if required (optional)

创建标识组和用户

步骤1.导航给**Administration >身份管理> Groups >用户标识组。**

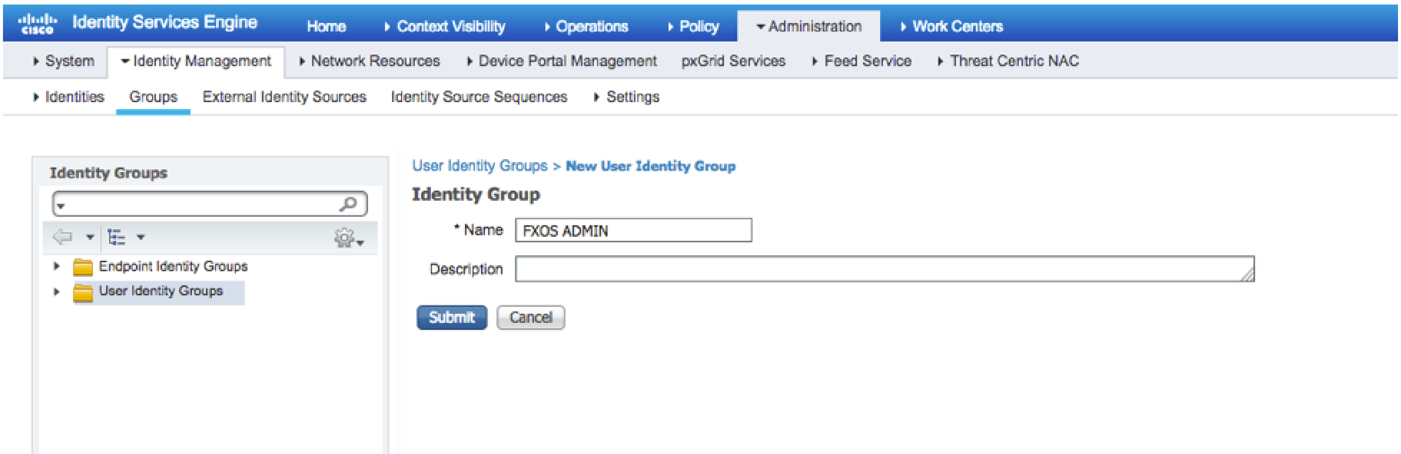
步骤2.单击**添加。**



User Identity Groups

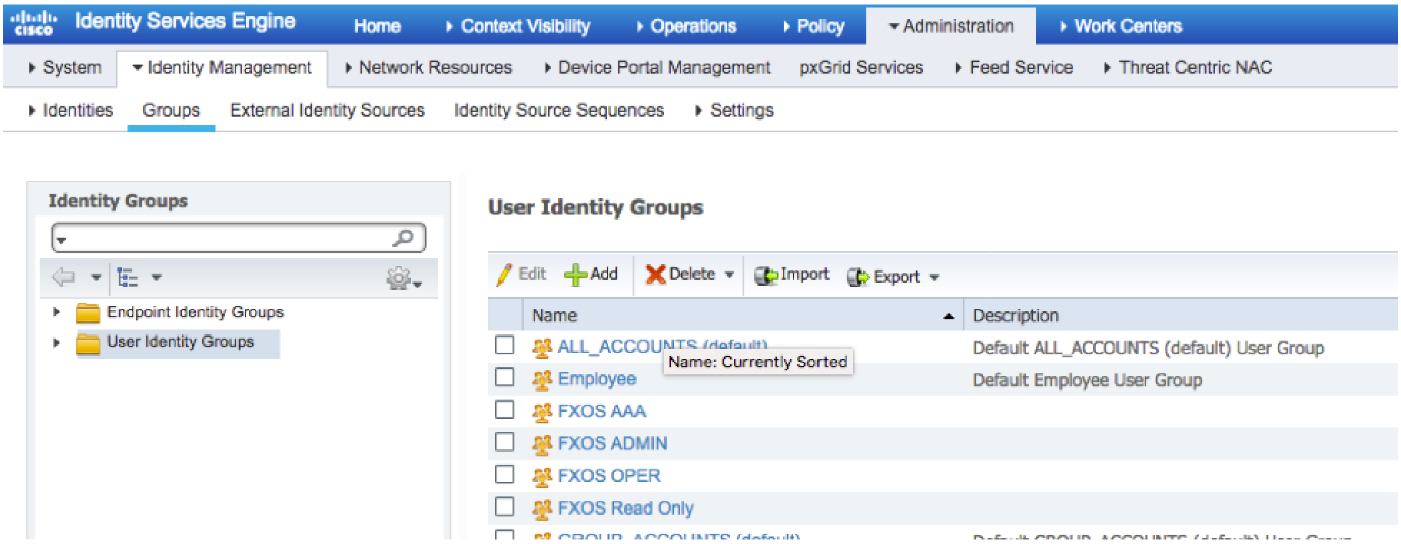
Name	Description
□ ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
□ Employee	Default Employee User Group
□ GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
□ GuestType_Contractor (default)	Identity group mirroring the guest type
□ GuestType_Daily (default)	Identity group mirroring the guest type
□ GuestType_Weekly (default)	Identity group mirroring the guest type
□ OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

步骤3.输入名称的值并且单击**提交。**



* Name	FXOS ADMIN
Description	

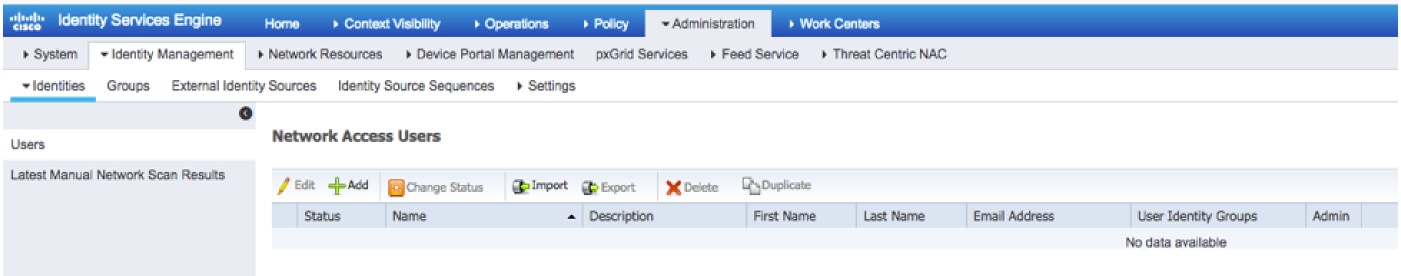
步骤4.重复所有所需的用户角色的步骤3。



	Name	Description
□	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
□	Employee	Default Employee User Group
□	FXOS AAA	
□	FXOS ADMIN	
□	FXOS OPER	
□	FXOS Read Only	
□	GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group

步骤5.导航对**Administration >身份管理>标识> Users。**

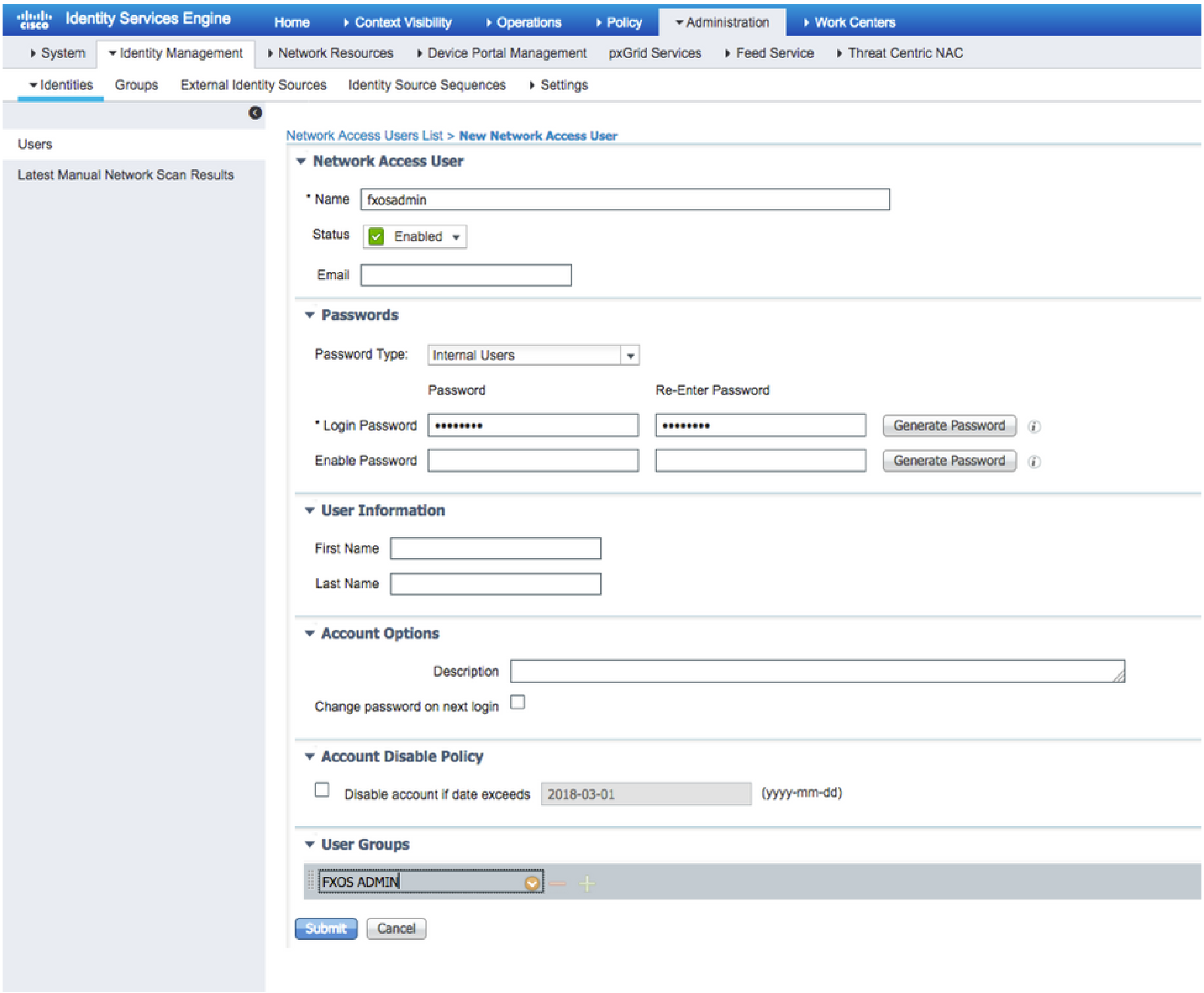
步骤6.单击**添加。**



Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin

No data available

步骤7.输入需要的值(名称、用户组，密码)。



Network Access Users List > **New Network Access User**

Network Access User

* Name: fxosadmin

Status: ☑ Enabled

Email:

Passwords

Password Type: Internal Users

	Password	Re-Enter Password	
* Login Password	••••••••	••••••••	Generate Password
Enable Password			Generate Password

User Information

First Name:

Last Name:

Account Options

Description:

Change password on next login □

Account Disable Policy

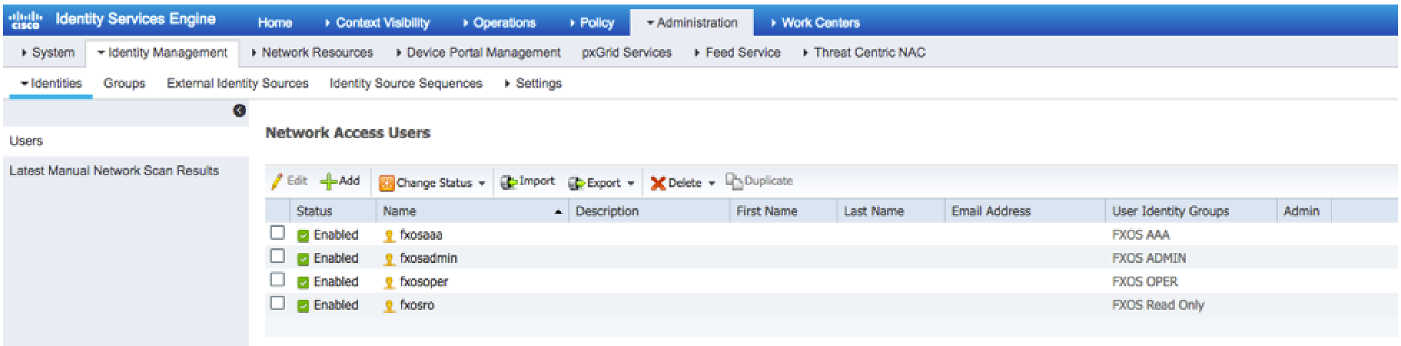
□ Disable account if date exceeds 2018-03-01 (yyyy-mm-dd)

User Groups

FXOS ADMIN

Submit Cancel

步骤8.重复全部必需用户的步骤6。

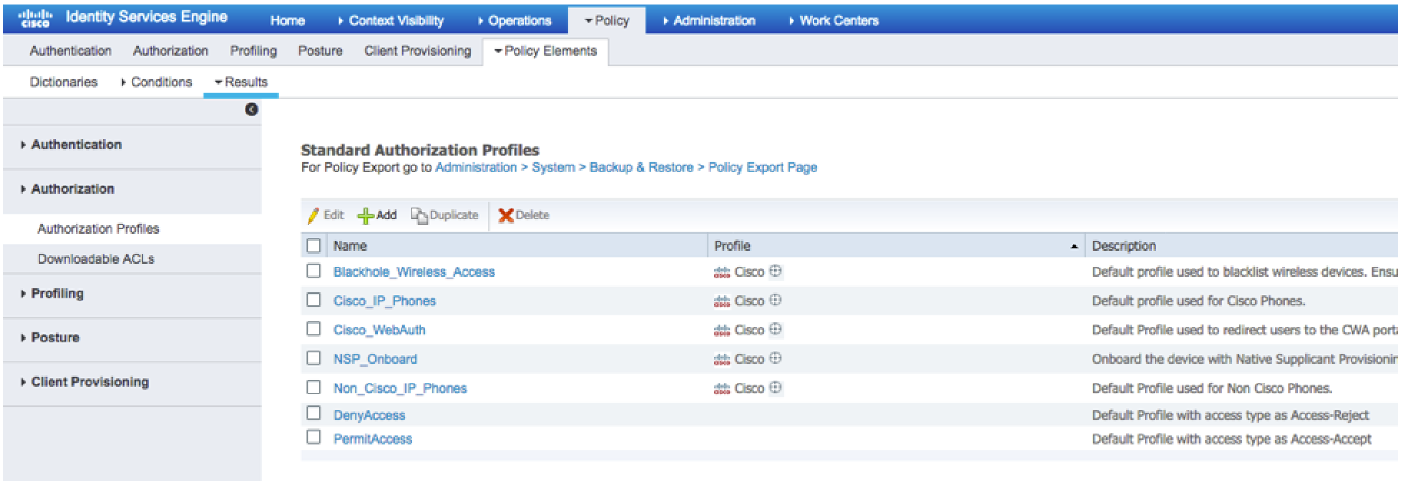


Network Access Users

	Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
□	☑ Enabled	fxosaaa					FXOS AAA	
□	☑ Enabled	fxosadmin					FXOS ADMIN	
□	☑ Enabled	fxosoper					FXOS OPER	
□	☑ Enabled	fxosro					FXOS Read Only	

创建每个用户角色的授权配置文件

步骤1.导航对**策略>Policy元素>结果>授权>授权配置文件。**



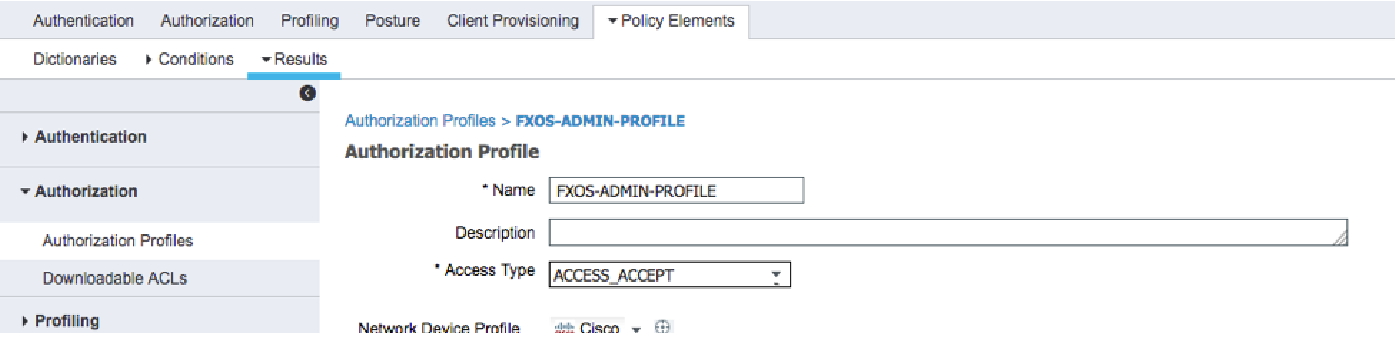
Standard Authorization Profiles

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

□	Name	Profile	Description
□	Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensu
□	Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
□	Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA port
□	NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisionir
□	Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
□	DenyAccess		Default Profile with access type as Access-Reject
□	PermitAccess		Default Profile with access type as Access-Accept

步骤2.填装授权配置文件的所有属性。

2.1. 配置配置文件名称。



Authorization Profiles > FXOS-ADMIN-PROFILE

Authorization Profile

* Name: FXOS-ADMIN-PROFILE

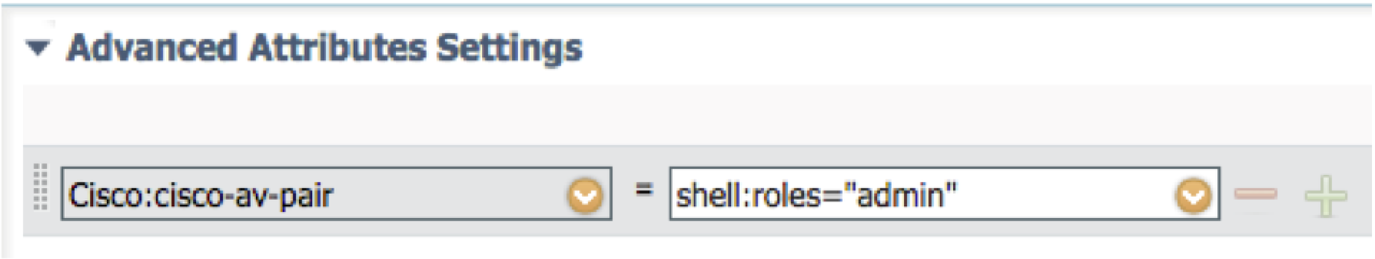
Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

2.2. 在**先进的属性设置请**配置以下CISCO-AV-PAIR

cisco-av-pair=shell ：roles= " admin”



Advanced Attributes Settings

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

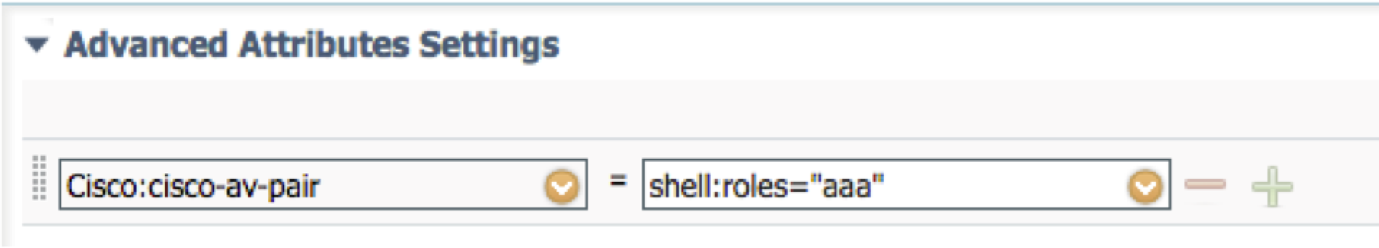
2.3. Click **Save**.

步骤3.使用以下Cisco AV对，重复剩余的用户角色的步骤2

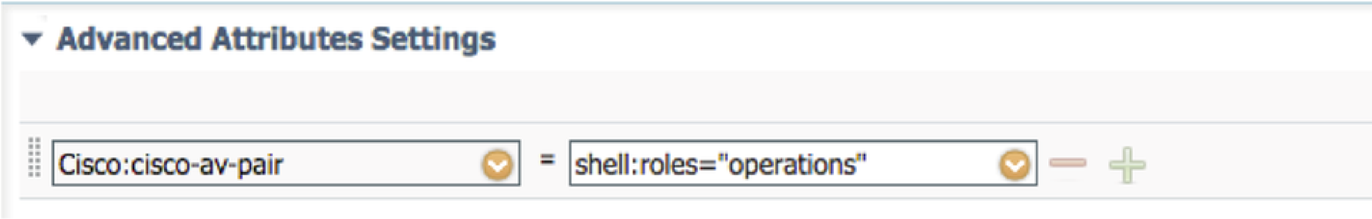
cisco-av-pair=shell ：roles= " aaa”

cisco-av-pair=shell ：roles= "操作”

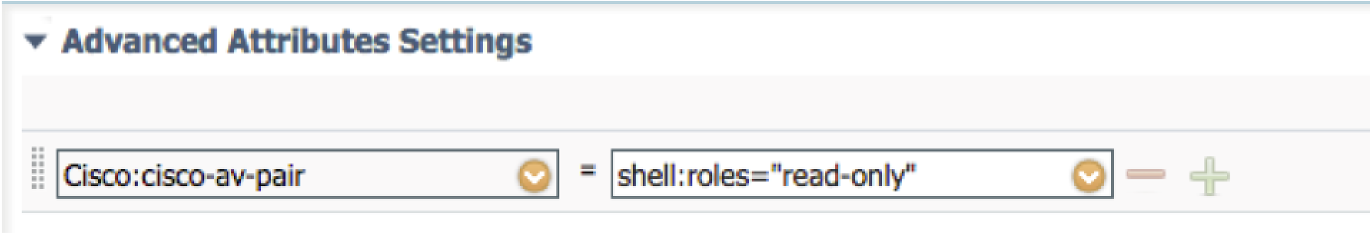
cisco-av-pair=shell ："只读”的roles=



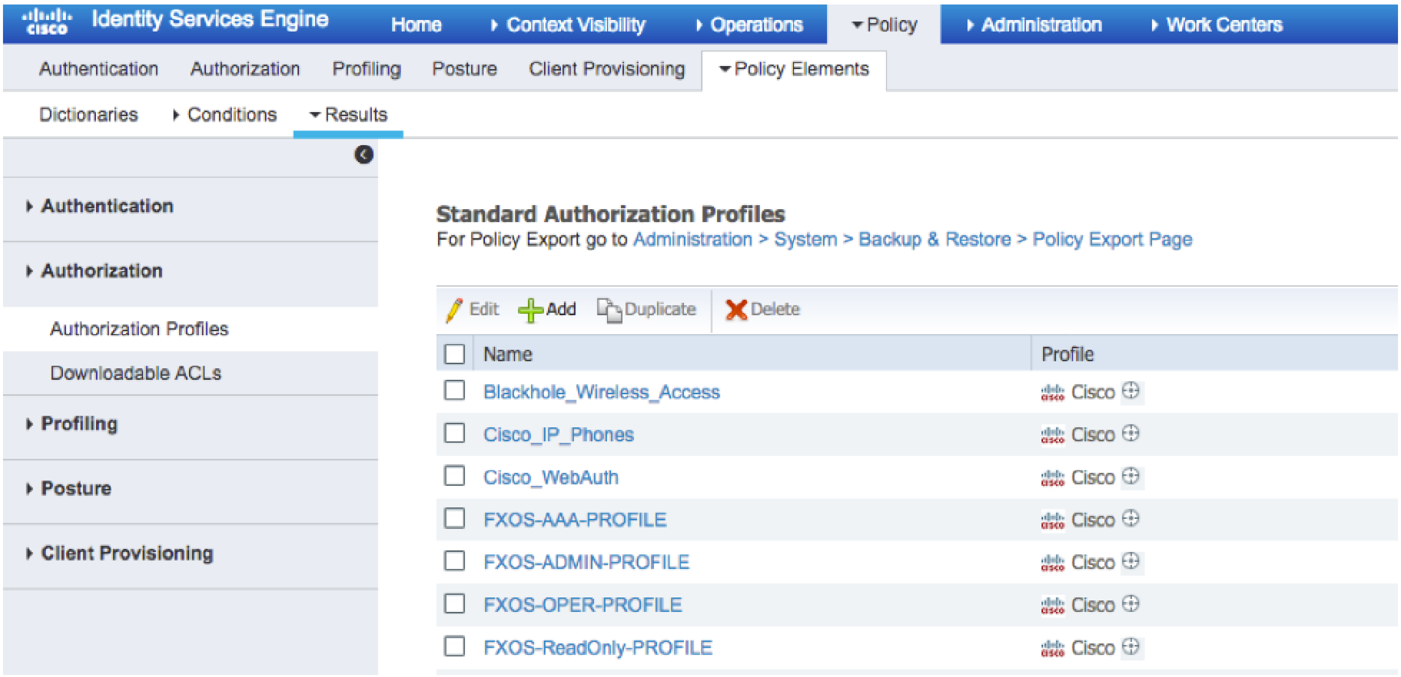
Cisco:cisco-av-pair = shell:roles="aaa"



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



Cisco:cisco-av-pair = shell:roles="read-only"



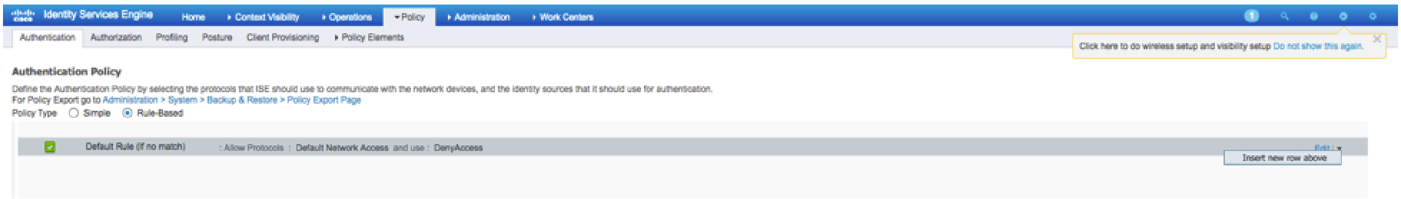
Standard Authorization Profiles

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

□	Name	Profile
□	Blackhole_Wireless_Access	Cisco
□	Cisco_IP_Phones	Cisco
□	Cisco_WebAuth	Cisco
□	FXOS-AAA-PROFILE	Cisco
□	FXOS-ADMIN-PROFILE	Cisco
□	FXOS-OPER-PROFILE	Cisco
□	FXOS-ReadOnly-PROFILE	Cisco

创建验证策略

步骤1.导航对**策略>验证>**并且单击箭头在旁边编辑您要创建规则的地方。


Identity Services Engine | Home | ▸ Context Visibility | ▸ Operations | ▾ Policy | ▸ Administration | ▸ Work Centers

Authentication | Authorization | Profiling | Posture | Client Provisioning | ▸ Policy Elements

Click here to do wireless setup and visibility setup Do not show this again.

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Policy Type ○ Simple ● Rule-Based

☑ Default Rule (If no match) : Allow Protocols : Default Network Access and use : DenyAccess

Edit | ▾ Insert new row above

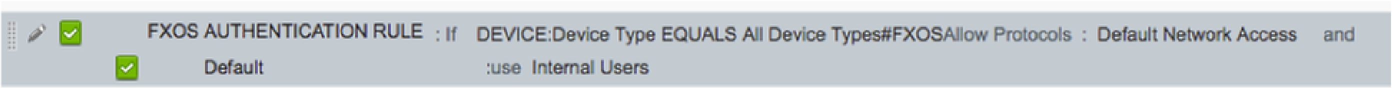
第二步：设置简单;它可以是执行的更加粒状，但是对于此示例我们将使用设备类型：

名称：**FXO验证规则**

IF挑选新团体/值：**设备：设备类型等于所有设备类型#FXOS**

允许协议：默认网络网络访问

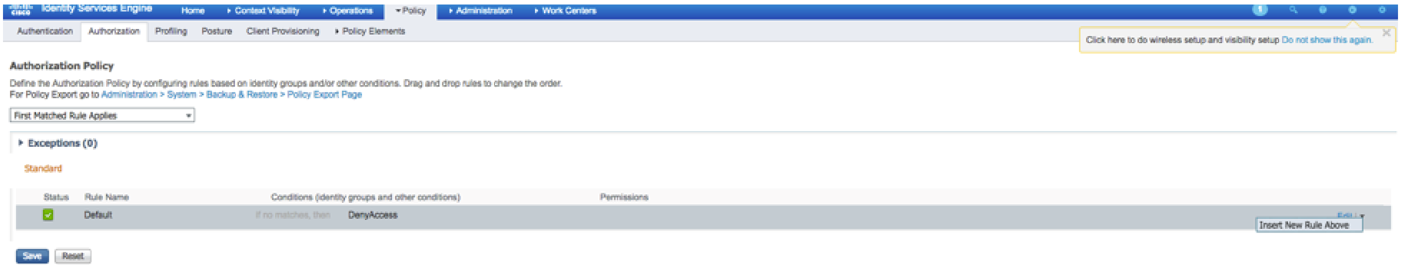
使用：内部用户


☑ FXOS AUTHENTICATION RULE : If DEVICE:Device Type EQUALS All Device Types#FXOSAllow Protocols : Default Network Access and

☑ Default :use Internal Users

创建授权策略

步骤1.导航对**策略>授权>**并且点击箭头网编辑您要创建规则的地方。


Identity Services Engine | Home | ▸ Context Visibility | ▸ Operations | ▾ Policy | ▸ Administration | ▸ Work Centers

Authentication | Authorization | Profiling | Posture | Client Provisioning | ▸ Policy Elements

Click here to do wireless setup and visibility setup Do not show this again.

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies ▾

▸ Exceptions (0)

Standard

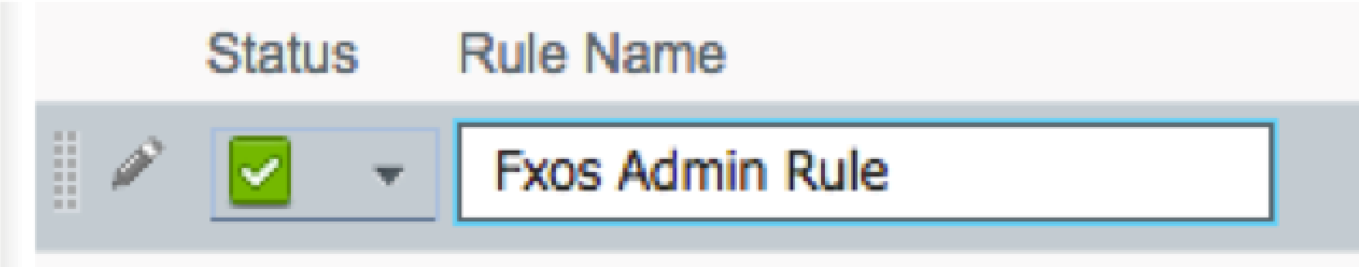
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
☑	Default	if no matches, then	DenyAccess

Edit | ▾ Insert New Rule Above

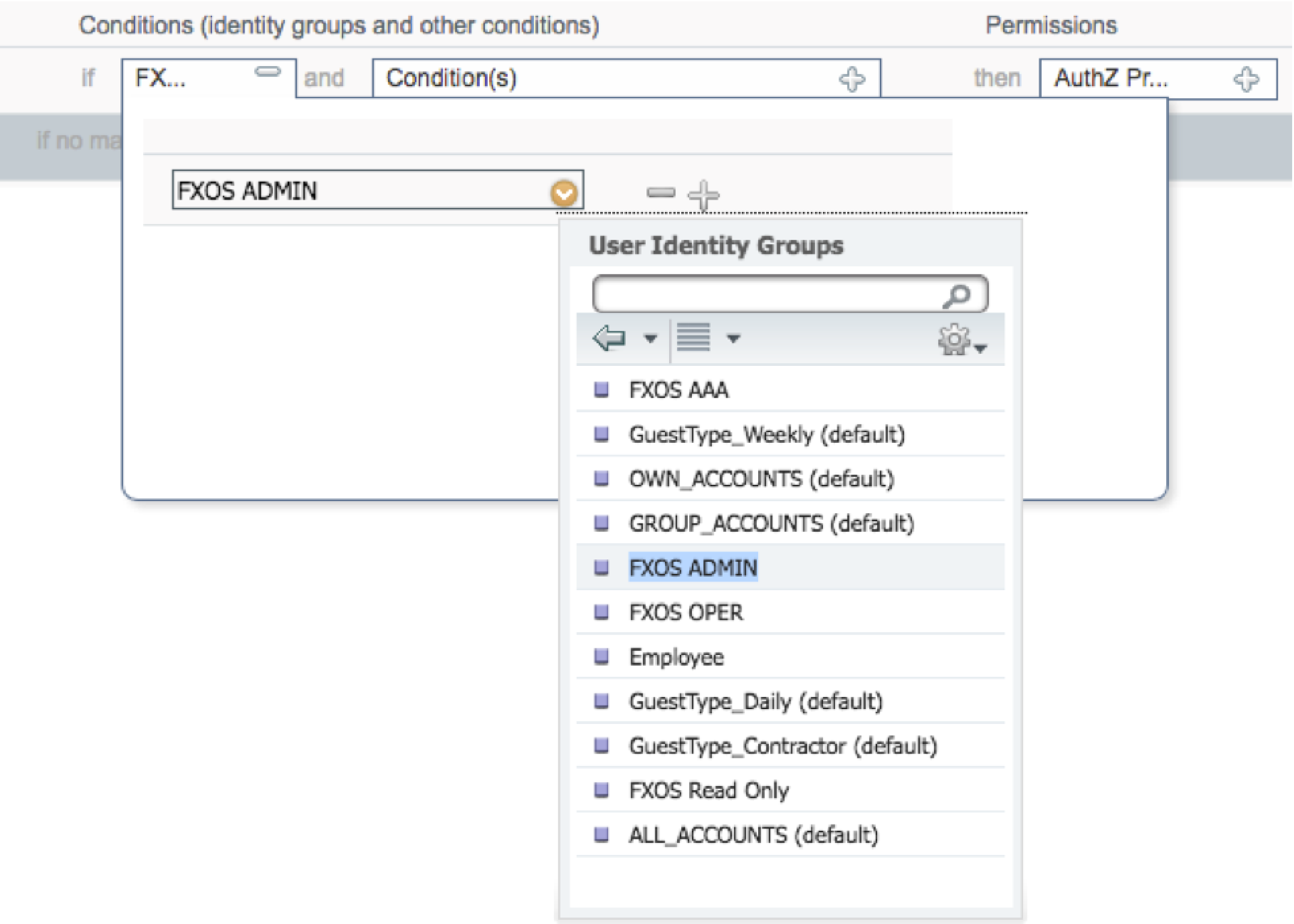
Save Reset

步骤2.输入授权规则的值与要求的参数。

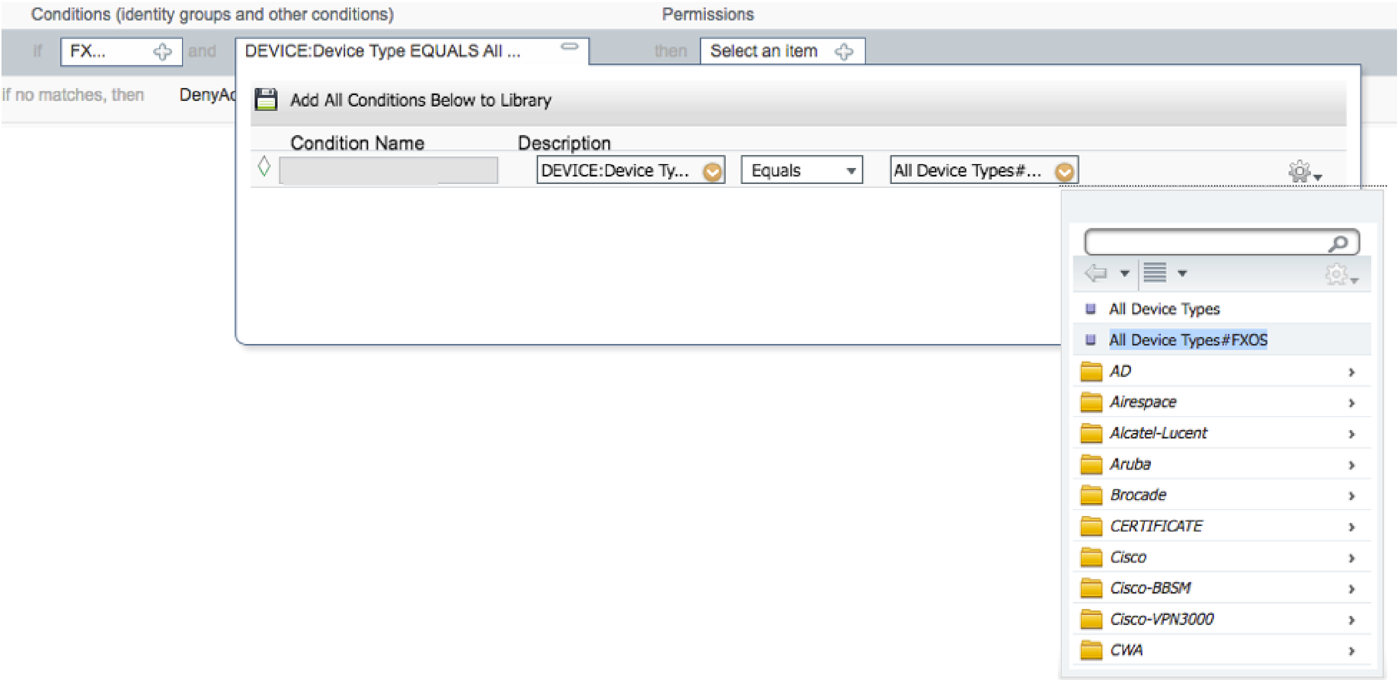
2.1. 规则名称：**Fxos <USER ROLE>规则。**


Status	Rule Name
☑ ▾	Fxos Admin Rule

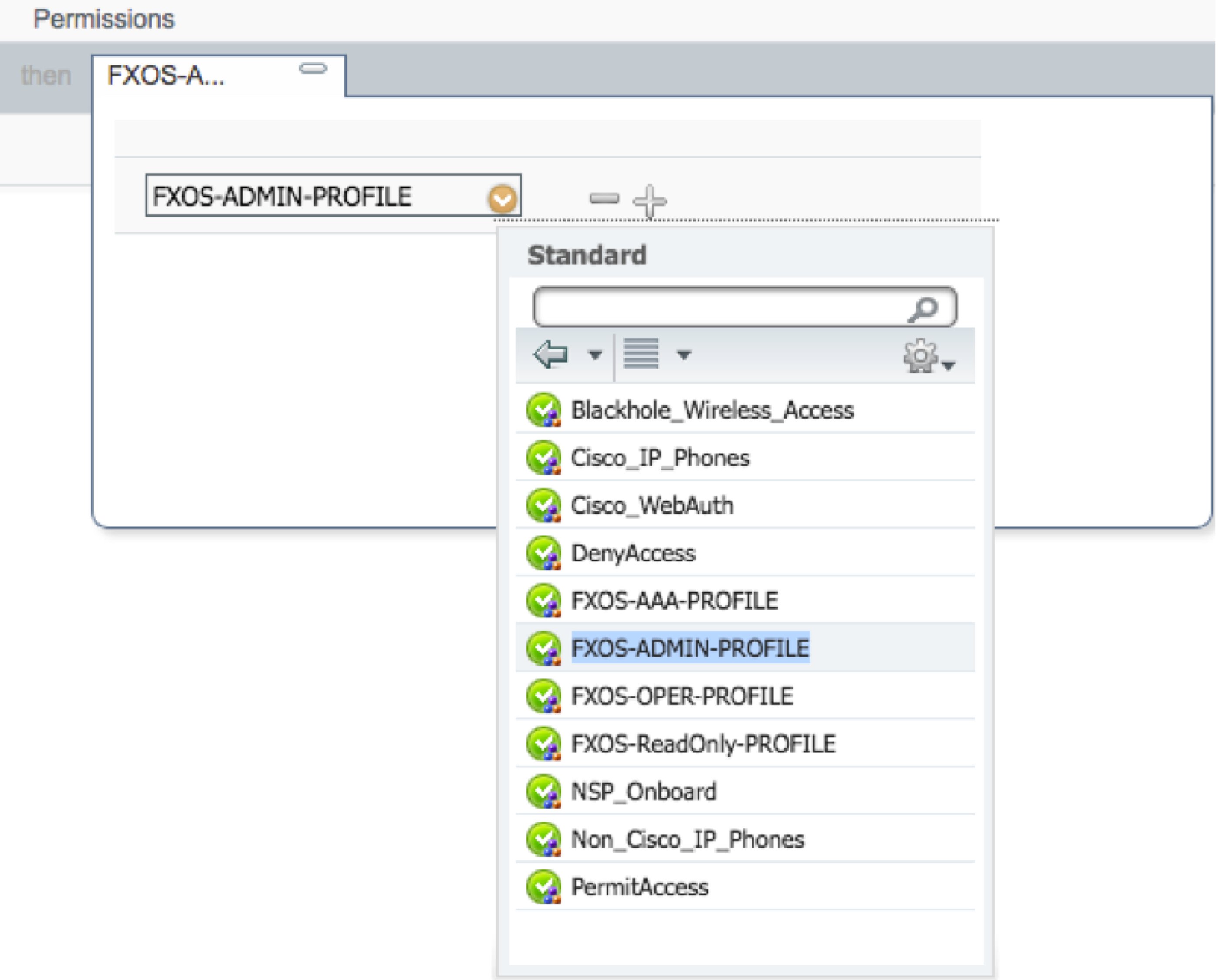
2.2. 如果：用户标识Groups>挑选<USER **ROLE>**。

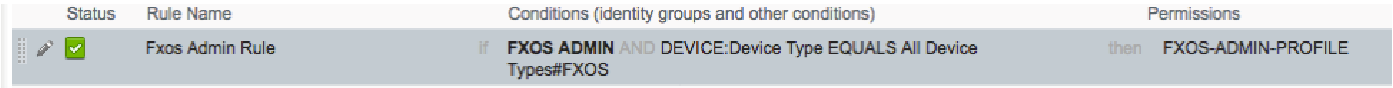


2.3. 并且：创建新的情况>设备：设备类型等于**所有设备类型#FXOS。**



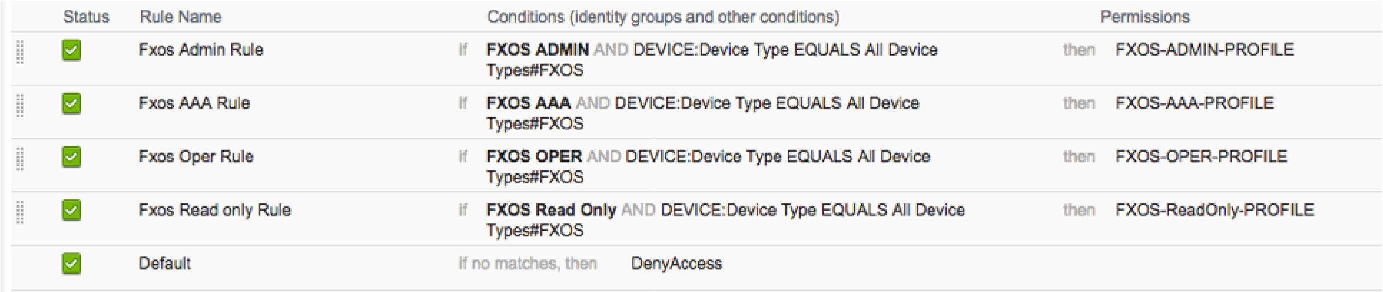
2.4. 权限：英文虎报>选择**用户角色配置文件**





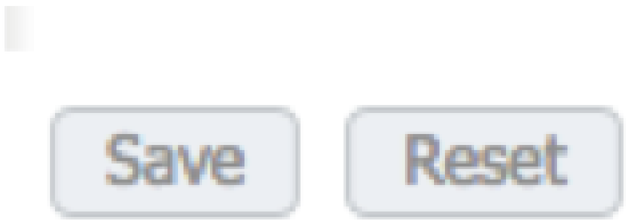
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Fxos Admin Rule	if	**FXOS ADMIN** AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	FXOS-ADMIN-PROFILE

步骤3.重复所有用户角色的步骤2。



Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Fxos Admin Rule	if	**FXOS ADMIN** AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	FXOS-ADMIN-PROFILE
✓	Fxos AAA Rule	if	**FXOS AAA** AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	FXOS-AAA-PROFILE
✓	Fxos Oper Rule	if	**FXOS OPER** AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	FXOS-OPER-PROFILE
✓	Fxos Read only Rule	if	**FXOS Read Only** AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	FXOS-ReadOnly-PROFILE
✓	Default	if no matches, then	DenyAccess		

步骤4.单击**“Save”**在页底端。



验证

您可以当前测试每个用户和验证已分配用户角色。

FXO机箱验证

1. Telnet或SSH对FXO机箱和登录使用任何已创建用户ISE的。

```
用户名：fxosadmin

密码：

fpr4120-TAC-A#范围安全

fpr4120-TAC-A /security #显示远程用户详细信息

远程用户fxosaaa ：

  说明：

  用户角色：

     名称：aaa

     名称：只读

远程用户fxosadmin ：

  说明：

  用户角色：

     名称：admin

     名称：只读

远程用户fxosoper ：

  说明：

  用户角色：

     名称：操作
```

名称：**只读**

远程用户**fxosro** ：

说明：

用户角色：

名称：**只读**

根据输入FXO机箱cli的用户名只将显示为用户角色授权的命令分配。

管理员用户角色。

```
fpr4120-TAC-A /security # ?
 确认确认
 结算用户塞申斯Clear user塞申斯
 创建创建托管对象
 删除删除托管对象
 禁用功能失效服务
 enable (event)启用服务
 回车输入托管对象
 范围更改电流模式
 设置集合属性值
 显示Show system information
 终止激活cimc会话
fpr4120-TAC-A#连接fxos
fpr4120-TAC-A (fxos) # debug aaa AAA请求
fpr4120-TAC-A (fxos) #
```

只读用户角色。

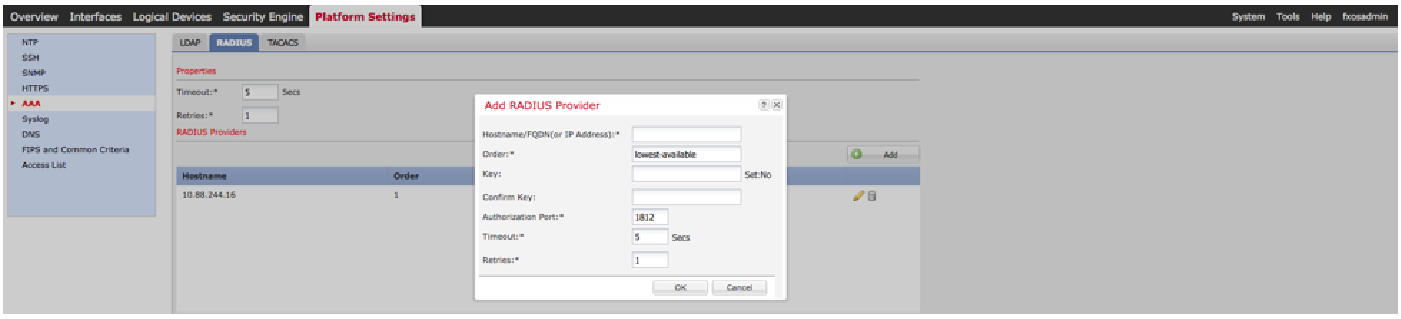
```
fpr4120-TAC-A /security # ?
 范围更改电流模式
 设置集合属性值
 显示Show system information
```

fpr4120-TAC-A#**连接fxos**

fpr4120-TAC-A (fxos) # **debug aaa AAA请求**

%为角色拒绝的权限

2. 使用任何ISE的，已创建用户浏览对FXO机箱IP地址和登录。
管理员用户角色。



Properties

Timeout:* 5 Secs

Retries:* 1

RADIUS Providers

Hostname	Order
10.88.244.16	1

Add RADIUS Provider

Hostname/FQDN(or IP Address):*

Order:* lowest-available

Key: Set:No

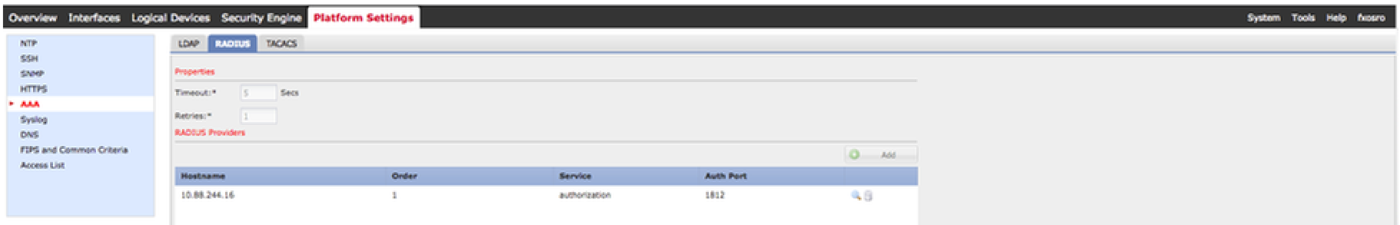
Confirm Key:

Authorization Port:* 1812

Timeout:* 5 Secs

Retries:* 1

只读用户角色。



Properties

Timeout:* 5 Secs

Retries:* 1

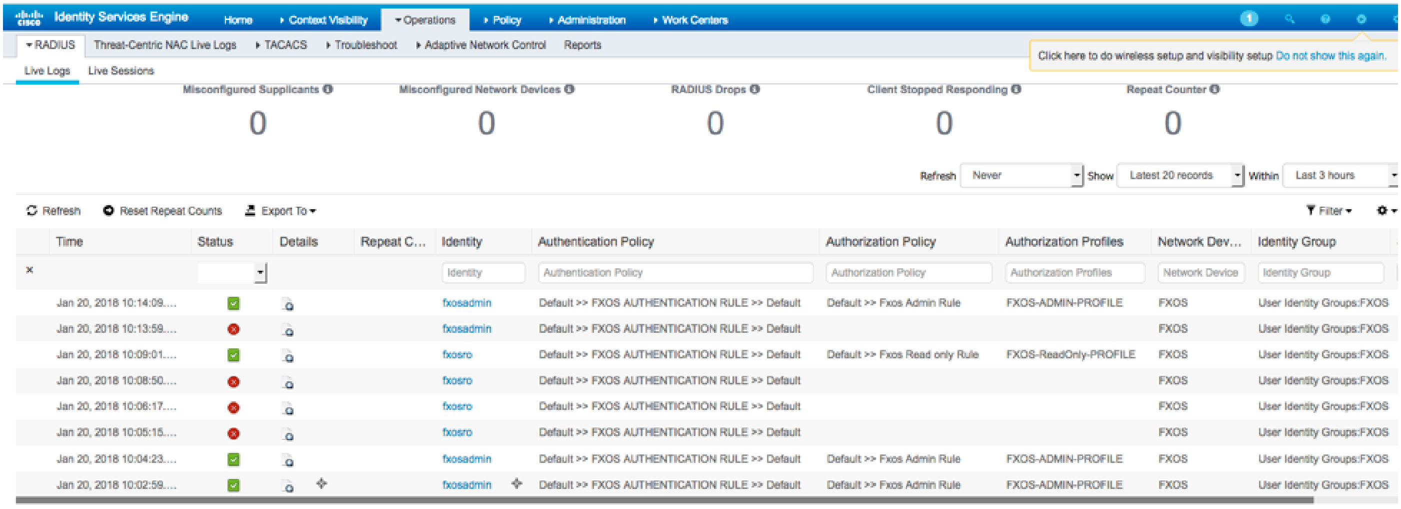
RADIUS Providers

Hostname	Order	Service	Auth Port
10.88.244.16	1	authorization	1812

Note:注意**Add按钮**变灰。

ISE 2.0验证

1. 导航对**操作> RADIUS> Live日志。**您应该能发现成功和失败的尝试。



Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 0

Repeat Counter 0

Refresh Never | Show Latest 20 records | Within Last 3 hours

Time	Status	Details	Repeat C...	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Network Dev...	Identity Group
Jan 20, 2018 10:14:09....	✓			fxosadmin	Default >> FXOS AUTHENTICATION RULE >> Default	Default >> Fxos Admin Rule	FXOS-ADMIN-PROFILE	FXOS	User Identity Groups:FXOS
Jan 20, 2018 10:13:59....	✗			fxosadmin	Default >> FXOS AUTHENTICATION RULE >> Default			FXOS	User Identity Groups:FXOS
Jan 20, 2018 10:09:01....	✓			fxosro	Default >> FXOS AUTHENTICATION RULE >> Default	Default >> Fxos Read only Rule	FXOS-ReadOnly-PROFILE	FXOS	User Identity Groups:FXOS
Jan 20, 2018 10:08:50....	✗			fxosro	Default >> FXOS AUTHENTICATION RULE >> Default			FXOS	User Identity Groups:FXOS
Jan 20, 2018 10:06:17....	✗			fxosro	Default >> FXOS AUTHENTICATION RULE >> Default			FXOS	User Identity Groups:FXOS
Jan 20, 2018 10:05:15....	✗			fxosro	Default >> FXOS AUTHENTICATION RULE >> Default			FXOS	User Identity Groups:FXOS
Jan 20, 2018 10:04:23....	✓			fxosadmin	Default >> FXOS AUTHENTICATION RULE >> Default	Default >> Fxos Admin Rule	FXOS-ADMIN-PROFILE	FXOS	User Identity Groups:FXOS
Jan 20, 2018 10:02:59....	✓			fxosadmin	Default >> FXOS AUTHENTICATION RULE >> Default	Default >> Fxos Admin Rule	FXOS-ADMIN-PROFILE	FXOS	User Identity Groups:FXOS

故障排除

为了debug aaa authentication和授权运行以下in命令FXO cli。

```
fpr4120-TAC-A#连接fxos

fpr4120-TAC-A (fxos) # debug aaa AAA请求

fpr4120-TAC-A (fxos) # debug aaa事件

fpr4120-TAC-A (fxos) # debug aaa错误

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

在成功认证尝试，您将看到以下输出后。

```
2018简20 17:18:02.410275 aaa ：验证的aaa_req_process。会话没有0

2018简20 17:18:02.410297 aaa ：aaa_req_process ：常规从appln的AAA请求：登录
appln_subtype ：默认

2018简20 17:18:02.410310 aaa ：try_next_aaa_method

2018简20 17:18:02.410330 aaa ：配置的总方法是1，将尝试的当前索引是0

2018简20 17:18:02.410344 aaa ：handle_req_using_method

2018简20 17:18:02.410356 aaa ：AAA_METHOD_SERVER_GROUP

2018简20 17:18:02.410367 aaa ：aaa_sg_method_handler group= radius

2018简20 17:18:02.410379 aaa ：使用通过对此功能的sg_protocol

2018简20 17:18:02.410393 aaa ：发送请求对RADIUS服务

2018简20 17:18:02.412944 aaa ：mts_send_msg_to_prot_daemon ：有效载荷长度= 374

2018简20 17:18:02.412973 aaa ：会话：0x8dfd68c被添加到会话表1

2018简20 17:18:02.412987 aaa ：已配置的方法组继之后

2018简20 17:18:02.656425 aaa ：aaa_process_fd_set

2018简20 17:18:02.656447 aaa ：aaa_process_fd_set ：在aaa_q的mtscallback

2018简20 17:18:02.656470 aaa ：mts_message_response_handler ：mts答复

2018简20 17:18:02.656483 aaa ：prot_daemon_reponse_handler

2018简20 17:18:02.656497 aaa ：会话：从会话表删除的0x8dfd68c 0

2018简20 17:18:02.656512 aaa ：is_aaa_resp_status_success状态= 1

2018简20 17:18:02.656525 aaa ：is_aaa_resp_status_success真

2018简20 17:18:02.656538 aaa ：验证的aaa_send_client_response。session-
>flags=21.aaa_resp->flags=0.
```

```
2018简20 17:18:02.656550 aaa ：AAA_REQ_FLAG_NORMAL

2018简20 17:18:02.656577 aaa ：成功的mts_send_response

2018简20 17:18:02.700520 aaa ：aaa_process_fd_set ：在aaa_accounting_q的mtscallback

2018简20 17:18:02.700688 aaa ：旧有操作码：accounting_interim_update

2018简20 17:18:02.700702 aaa ：aaa_create_local_acct_req ：user=， session_id=，
log=added用户fxosro

2018简20 17:18:02.700725 aaa ：核算的aaa_req_process。会话没有0

2018简20 17:18:02.700738 aaa ：MTS请求参考是NULL。本地请求

2018简20 17:18:02.700749 aaa ：设置AAA_REQ_RESPONSE_NOT_NEEDED

2018简20 17:18:02.700762 aaa ：aaa_req_process ：常规从appln的AAA请求：默认
appln_subtype ：默认

2018简20 17:18:02.700774 aaa ：try_next_aaa_method

2018简20 17:18:02.700798 aaa ：为默认默认配置的没有方法

2018简20 17:18:02.700810 aaa ：此请求的没有配置联机

2018简20 17:18:02.700997 aaa ：核算的aaa_send_client_response。session-
>flags=254.aaa_resp->flags=0.

2018简20 17:18:02.701010 aaa ：旧有库认为的请求的答复将被发送作为成功

2018简20 17:18:02.701021 aaa ：为此请求没需要的答复

2018简20 17:18:02.701033 aaa ：AAA_REQ_FLAG_LOCAL_RESP

2018简20 17:18:02.701044 aaa ：aaa_cleanup_session

2018简20 17:18:02.701055 aaa ：应该释放aaa_req。

2018简20 17:18:02.701067 aaa ：后退成功的方法本地

2018简20 17:18:02.706922 aaa ：aaa_process_fd_set

2018简20 17:18:02.706937 aaa ：aaa_process_fd_set ：在aaa_accounting_q的mtscallback

2018简20 17:18:02.706959 aaa ：旧有操作码：accounting_interim_update

2018简20 17:18:02.706972 aaa ：aaa_create_local_acct_req ：user=， session_id=，
log=added用户：对角色的fxosro ：只读
```

在失败的认证尝试，您将看到以下输出后。

```
2018简20 17:15:18.102130 aaa ：aaa_process_fd_set
```

```
2018简20 17:15:18.102149 aaa ：aaa_process_fd_set ：在aaa_q的mtscallback

2018简20 17:15:18.102267 aaa ：aaa_process_fd_set

2018简20 17:15:18.102281 aaa ：aaa_process_fd_set ：在aaa_q的mtscallback

2018简20 17:15:18.102363 aaa ：aaa_process_fd_set

2018简20 17:15:18.102377 aaa ：aaa_process_fd_set ：在aaa_q的mtscallback

2018简20 17:15:18.102456 aaa ：aaa_process_fd_set

2018简20 17:15:18.102468 aaa ：aaa_process_fd_set ：在aaa_q的mtscallback

2018简20 17:15:18.102489 aaa ：mts_aaa_req_process

2018简20 17:15:18.102503 aaa ：验证的aaa_req_process。会话没有0

2018简20 17:15:18.102526 aaa ：aaa_req_process ：常规从appln的AAA请求：登录
appln_subtype ：默认

2018简20 17:15:18.102540 aaa ：try_next_aaa_method

2018简20 17:15:18.102562 aaa ：配置的总方法是1，将尝试的当前索引是0

2018简20 17:15:18.102575 aaa ：handle_req_using_method

2018简20 17:15:18.102586 aaa ：AAA_METHOD_SERVER_GROUP

2018简20 17:15:18.102598 aaa ：aaa_sg_method_handler group= radius

2018简20 17:15:18.102610 aaa ：使用通过对此功能的sg_protocol

2018简20 17:15:18.102625 aaa ：发送请求对RADIUS服务

2018简20 17:15:18.102658 aaa ：mts_send_msg_to_prot_daemon ：有效载荷长度= 371

2018简20 17:15:18.102684 aaa ：会话：0x8dfd68c被添加到会话表1

2018简20 17:15:18.102698 aaa ：已配置的方法组继之后

2018简20 17:15:18.273682 aaa ：aaa_process_fd_set

2018简20 17:15:18.273724 aaa ：aaa_process_fd_set ：在aaa_q的mtscallback

2018简20 17:15:18.273753 aaa ：mts_message_response_handler ：mts答复

2018简20 17:15:18.273768 aaa ：prot_daemon_reponse_handler

2018简20 17:15:18.273783 aaa ：会话：从会话表删除的0x8dfd68c 0

2018简20 17:15:18.273801 aaa ：is_aaa_resp_status_success状态= 2
```

```
2018简20 17:15:18.273815 aaa ：is_aaa_resp_status_success真

2018简20 17:15:18.273829 aaa ：验证的aaa_send_client_response。session->flags=21.aaa_resp->flags=0.

2018简20 17:15:18.273843 aaa ：AAA_REQ_FLAG_NORMAL

2018简20 17:15:18.273877 aaa ：成功的mts_send_response

2018简20 17:15:18.273902 aaa ：aaa_cleanup_session

2018简20 17:15:18.273916 aaa ：请求数据mts_drop

2018简20 17:15:18.273935 aaa ：应该释放aaa_req。

2018简20 17:15:18.280416 aaa ：aaa_process_fd_set

2018简20 17:15:18.280443 aaa ：aaa_process_fd_set ：在aaa_q的mtscallback

2018简20 17:15:18.280454 aaa ：aaa_enable_info_config ：aaa登录错误消息的GET_REQ

2018简20 17:15:18.280460 aaa ：获得的上一步回归值配置运行：未知安全项目
```

相关信息

当TACACS/RADIUS验证启用， Ethanalyzer on命令FX-OS cli将提示输入密码的密码。此行为是由bug引起的。

Bug ID ： CSCvg87518