

# Firepower可擴展作業系統(FXOS)2.2:使用RADIUS通過ISE進行遠端管理的機箱身份驗證/授權

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[組態](#)

[配置FXOS機箱](#)

[配置ISE伺服器](#)

[驗證](#)

[FXOS機箱驗證](#)

[ISE 2.0驗證](#)

[疑難排解](#)

[相關資訊](#)

## 簡介

本檔案介紹如何透過身分識別服務引擎(ISE)設定Firepower可擴充作業系統(FXOS)機箱的RADIUS驗證和授權。

FXOS機箱包括以下使用者角色：

- Administrator — 對整個系統的完全讀寫訪問許可權。預設情況下為預設管理員帳戶分配此角色，並且無法更改。
- 只讀 — 對系統配置的唯一讀訪問許可權，無修改系統狀態的許可權。
- 操作 — 對NTP配置、智慧許可的Smart Call Home配置以及系統日誌（包括系統日誌伺服器和故障）的讀寫訪問許可權。對系統其餘部分的讀取訪問許可權。
- AAA — 對使用者、角色和AAA配置的讀寫訪問。對系統其餘部分的讀取訪問許可權。

通過CLI可以看到，如下所示：

```
fr4120-TAC-A /security* # show role
```

角色：

```
角色名稱Priv
```

```
-----
```

```
aaa aaa
```

admin

運營運營

唯讀唯讀

作者：Tony Ramirez、Jose Soto、Cisco TAC工程師。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- Firepower可擴展作業系統(FXOS)知識
- ISE配置知識

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Firepower 4120安全裝置版本2.2
- 虛擬思科身分識別服務引擎2.2.0.470

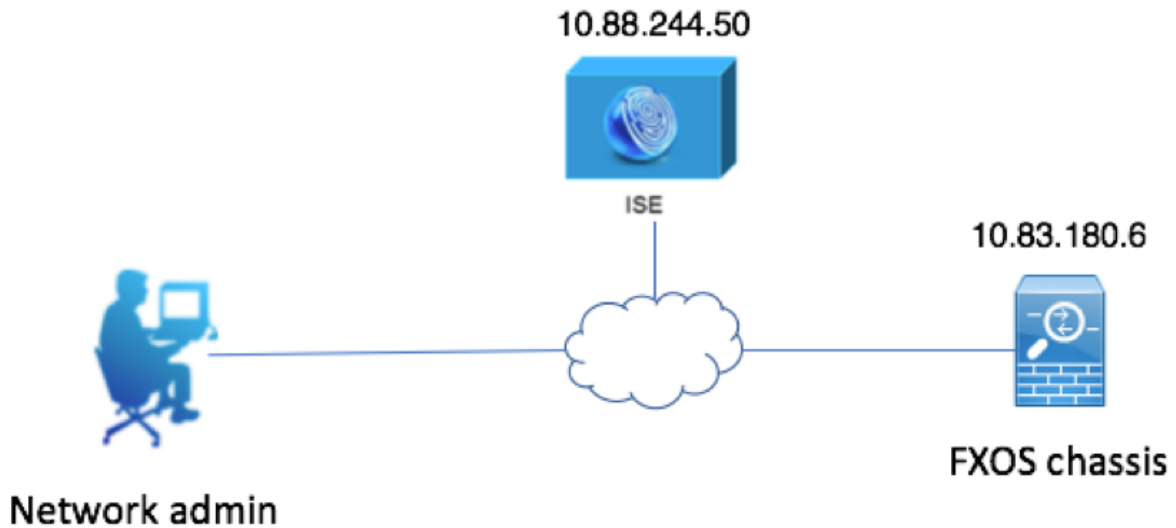
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 設定

此組態的目的是：

- 通過ISE驗證登入到FXOS基於Web的GUI和SSH的使用者
- 通過ISE根據使用者角色授權使用者登入FXOS基於Web的GUI和SSH。
- 通過ISE驗證FXOS上的身份驗證和授權操作是否正確

### 網路圖表



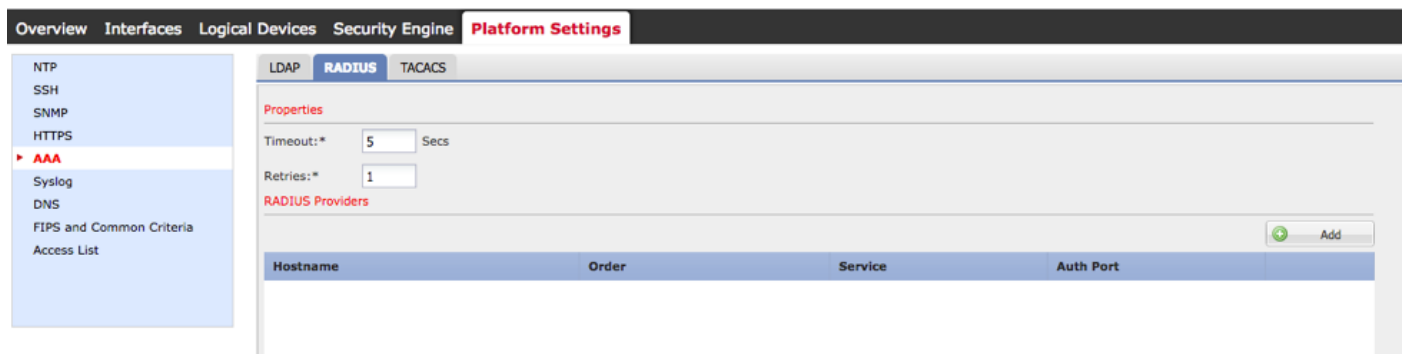
## 組態

### 配置FXOS機箱

使用機箱管理器建立RADIUS提供程式

步驟1.導覽至Platform Settings > AAA。

步驟2.按一下RADIUS索引標籤。

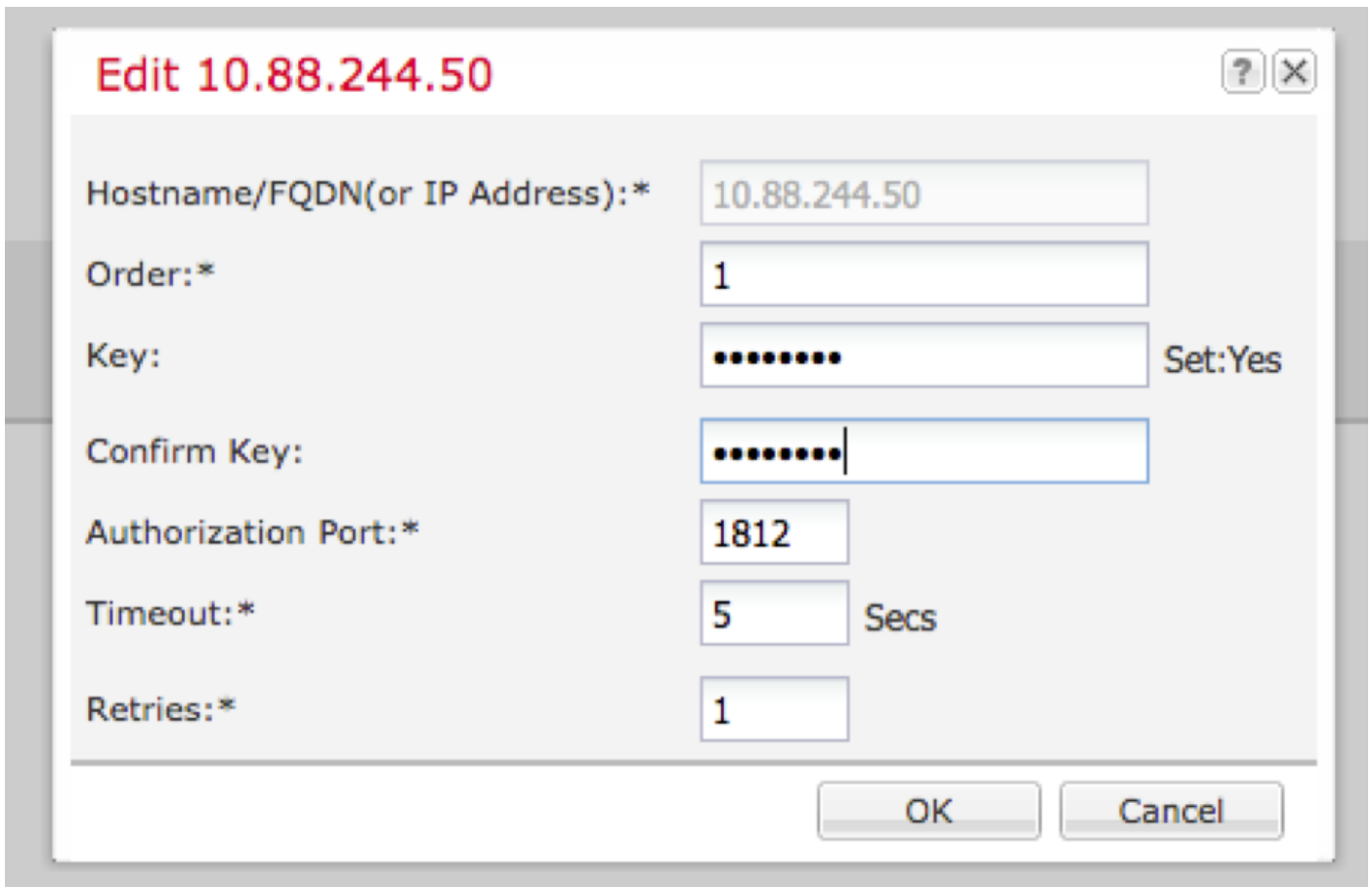


步驟3.對於要新增的每個RADIUS提供程式 ( 最多16個提供程式 )。

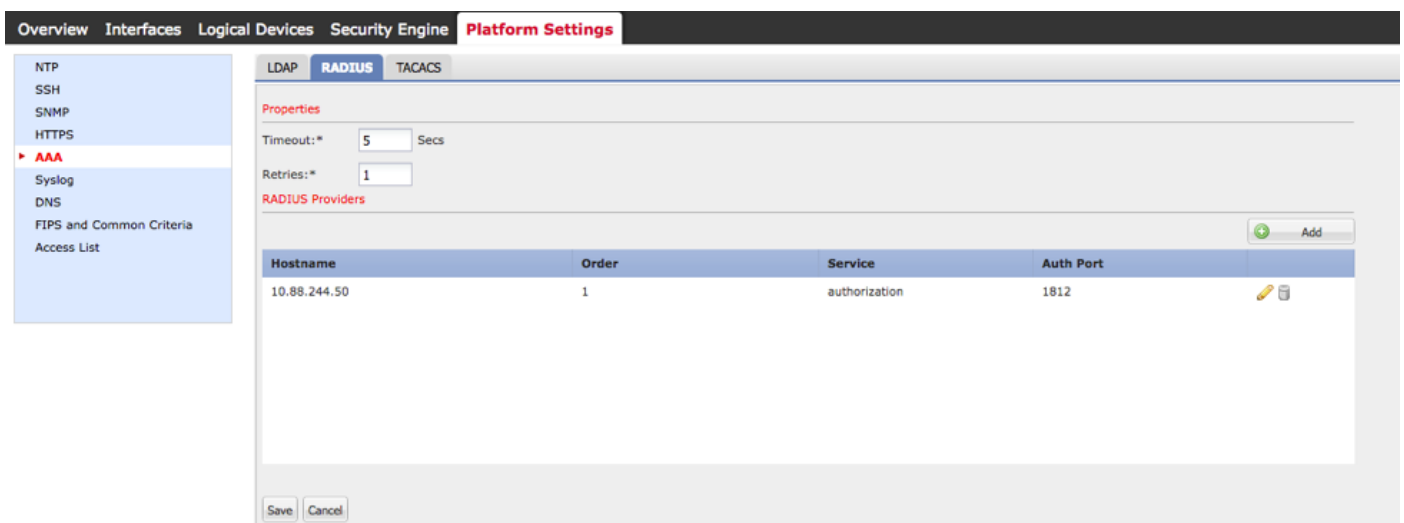
3.1.在RADIUS提供程式區域中，按一下Add。

3.2.開啟「新增RADIUS提供程式」對話方塊後，輸入所需的值。

3.3.按一下確定關閉「新增RADIUS提供程式」對話方塊。

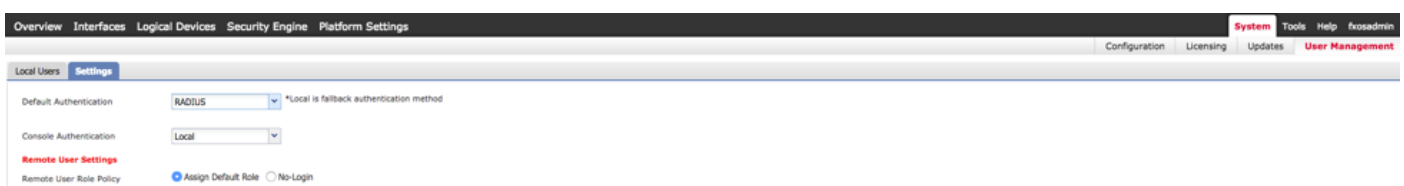


步驟4.按一下「Save」。



步驟5.導覽至System > User Management > Settings。

步驟6.在Default Authentication下選擇RADIUS。



使用CLI建立RADIUS提供程式

步驟1. 若要啟用RADIUS驗證，請運行以下命令。

```
fpr4120-TAC-A#作用域安全性
```

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

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

步驟2. 使用**show detail**命令顯示結果。

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

預設身份驗證：

管理領域：**Radius**

操作領域：**Radius**

Web會話刷新期間 ( 秒 )：600

Web、ssh、telnet會話的會話超時 ( 秒 )：600

Web、ssh、telnet會話的絕對會話超時 ( 秒 )：3600

串列控制檯會話超時 ( 秒 )：600

串列控制檯絕對會話超時 ( 秒 )：3600

管理員身份驗證伺服器組：

操作身份驗證伺服器組：

使用第二個因素：否

步驟3. 要配置RADIUS伺服器引數，請運行以下命令。

```
fpr4120-TAC-A#作用域安全性
```

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

```
fpr4120-TAC-A /security/radius # enter server 10.88.244.50
```

```
fpr4120-TAC-A /security/radius/server # set descr "ISE Server"
```

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

輸入金鑰：\*\*\*\*\*

確認金鑰：\*\*\*\*\*

步驟4. 使用**show detail**命令顯示結果。

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

RADIUS伺服器：

主機名、FQDN或IP地址：10.88.244.50

描述：

訂購：1

身份驗證埠：1812

主要:\*\*\*\*

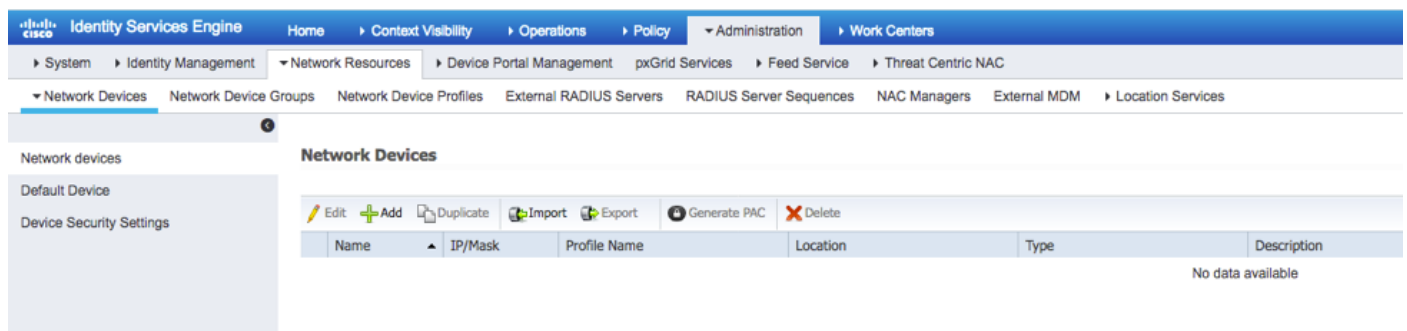
逾時:5

## 配置ISE伺服器

### 將FXOS新增為網路資源

步驟1.導覽至Administration > Network Resources > Network Devices。

步驟2.按一下ADD



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is Administration > Network Resources > Network Devices. The left sidebar shows the navigation menu with 'Network Devices' selected. The main content area displays the 'Network Devices' page with a table of devices. The table has columns for Name, IP/Mask, Profile Name, Location, Type, and Description. The table is currently empty, showing 'No data available'.

Name	IP/Mask	Profile Name	Location	Type	Description
No data available					

步驟3.輸入所需的值（名稱、IP地址、裝置型別和啟用RADIUS並新增金鑰），然後點選提交。

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

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 > New Network Device

**Network Devices**

\* Name

Description

---

\* IP Address:  /

---

\* Device Profile Cisco

Model Name

Software Version

---

\* Network Device Group

Device Type

IPSEC

Location

---

**RADIUS Authentication Settings**

**RADIUS UDP Settings**

Protocol **RADIUS**

\* Shared Secret

CoA Port

**RADIUS DTLS Settings** ⓘ

DTLS Required  ⓘ

Shared Secret  ⓘ

CoA Port

Issuer CA of ISE Certificates for CoA  ⓘ

## 建立身份組和使用者

步驟1. 導航到管理>身份管理>組>使用者身份組。

步驟2. 按一下ADD。

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

**Identity Groups**

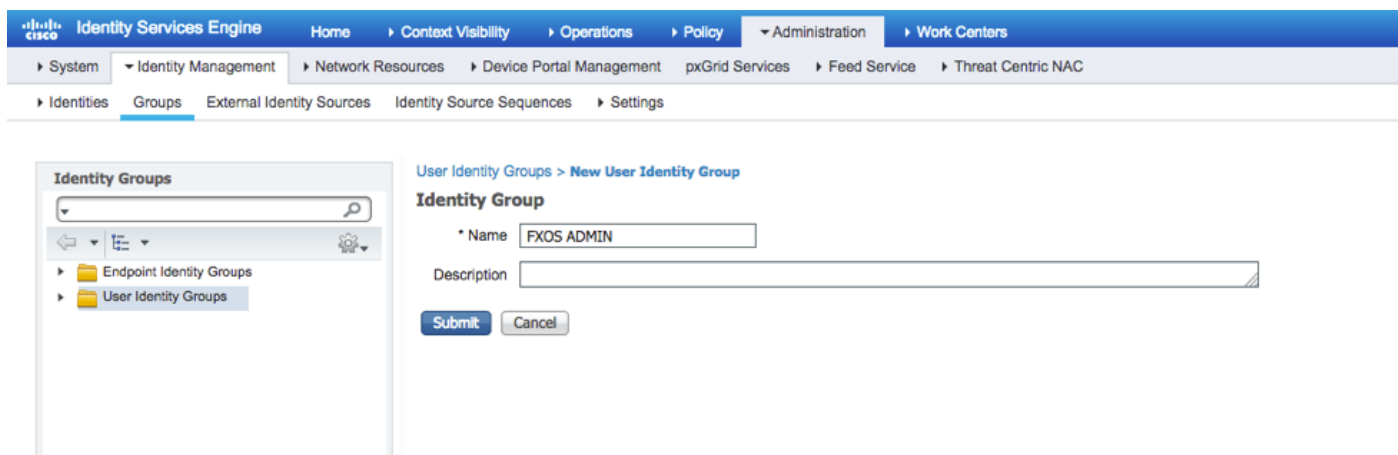
- Endpoint Identity Groups
- User Identity Groups**

**User Identity Groups**

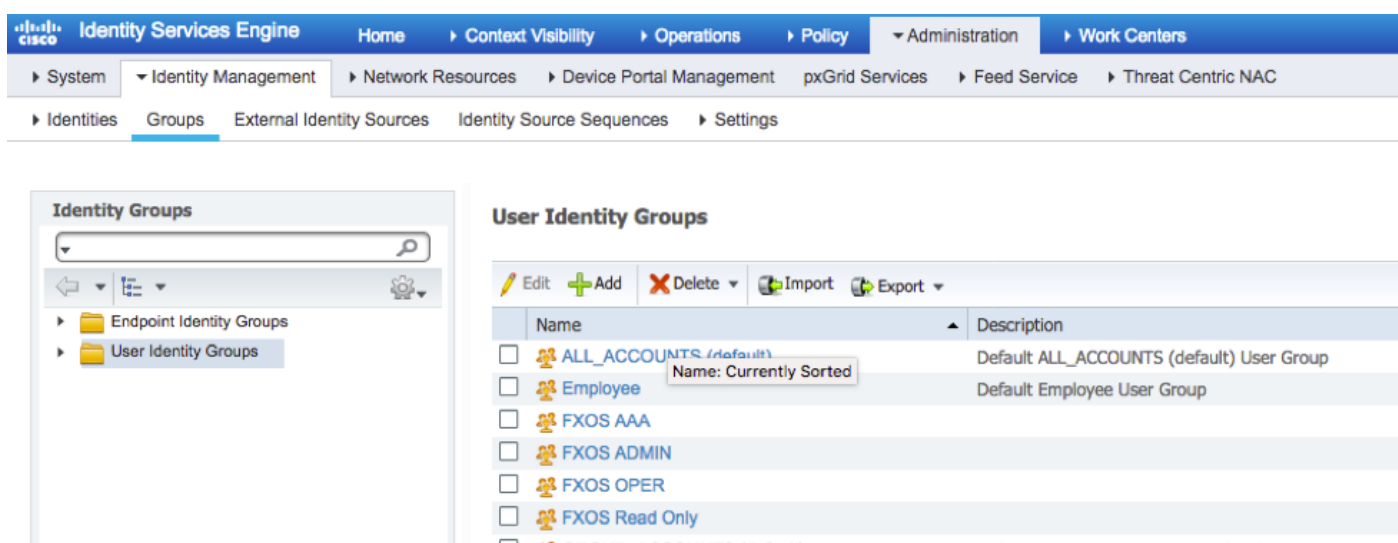
Edit  Add  Delete  Import  Export

<input type="checkbox"/>	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

步驟3.輸入Name的值，然後按一下Submit。

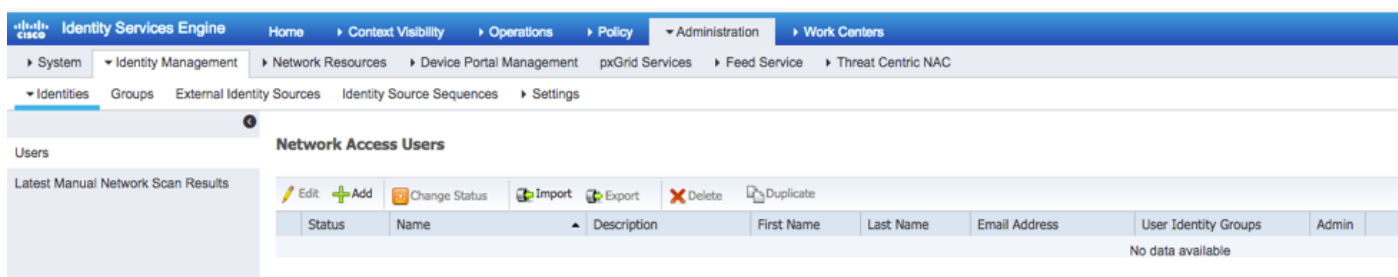


步驟4.對所有所需的使用者角色重複步驟3。



步驟5.導航到管理>身份管理>身份>使用者。

步驟6.按一下ADD。



步驟7.輸入所需的值（名稱、使用者組和密碼）。



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**

步驟8.對所有必需使用者重複步驟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

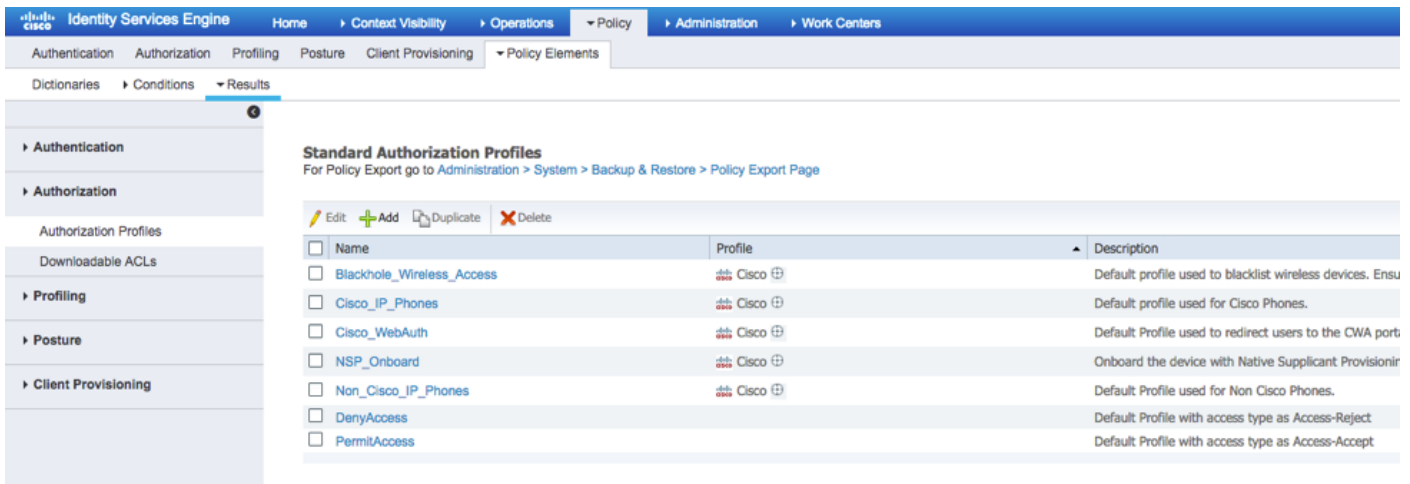
**Network Access Users**

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	

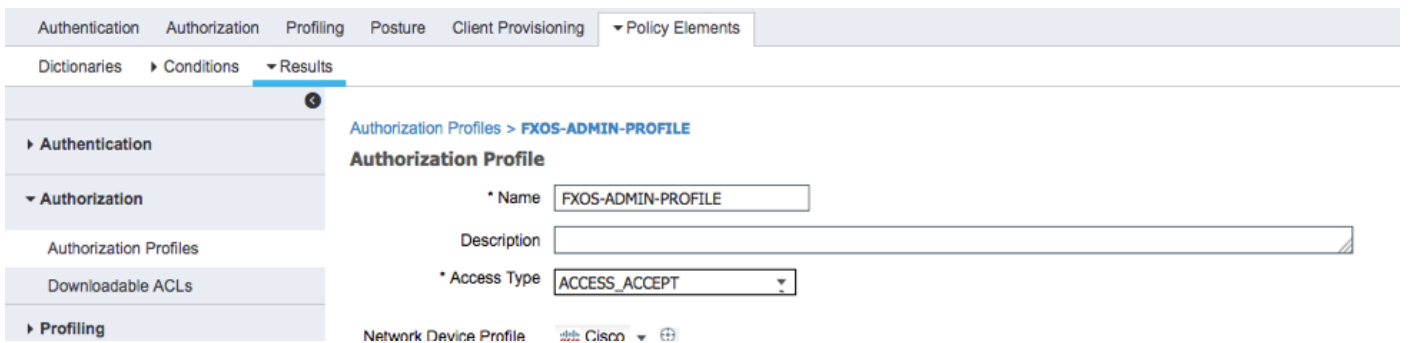
為每個使用者角色建立授權配置檔案

步驟1. 導覽至Policy > Policy Elements > Results > Authorization > Authorization Profiles。



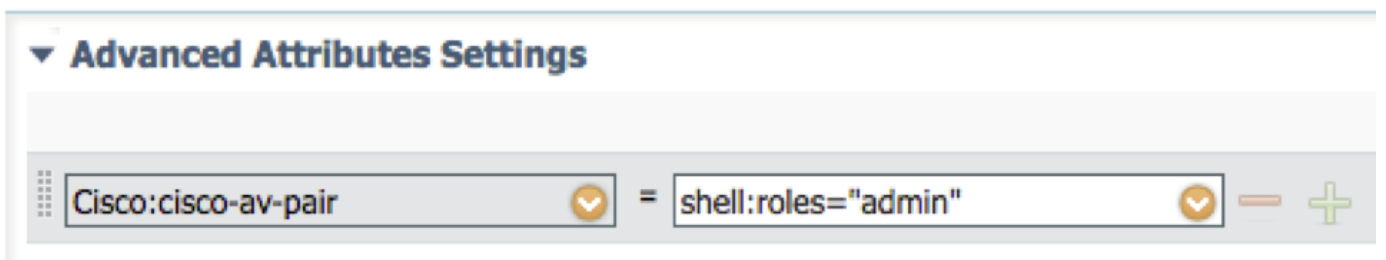
步驟2. 填充授權配置檔案的所有屬性。

### 2.1. 配置配置檔名稱。

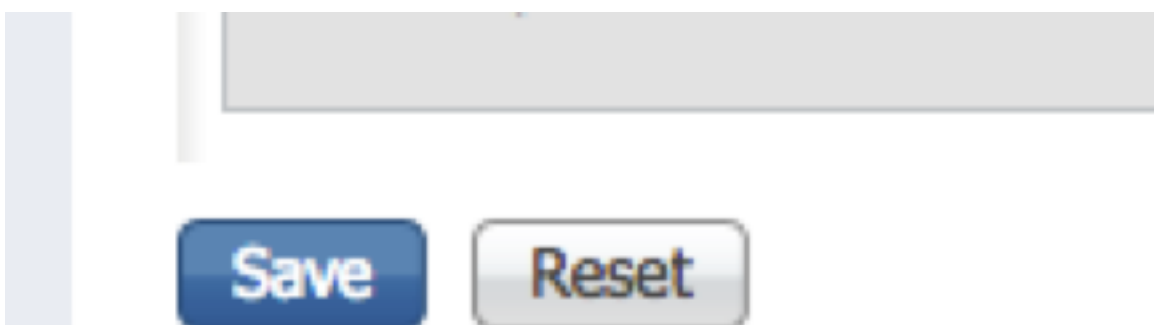


### 2.2. 在進階屬性設定中，設定以下CISCO-AV-PAIR

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



### 2.3. 按一下儲存。

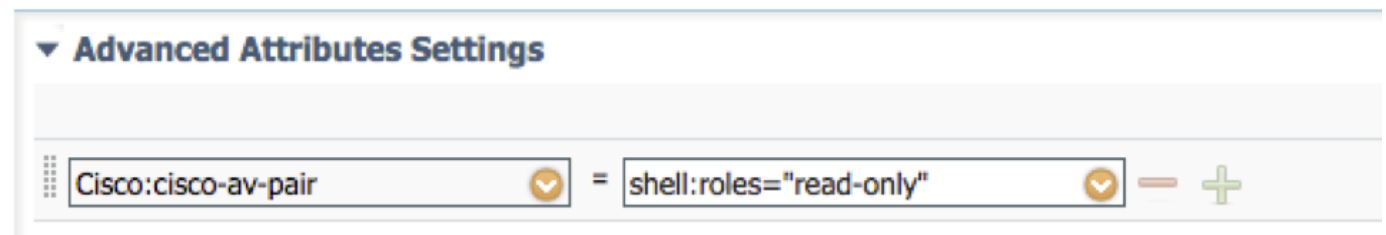
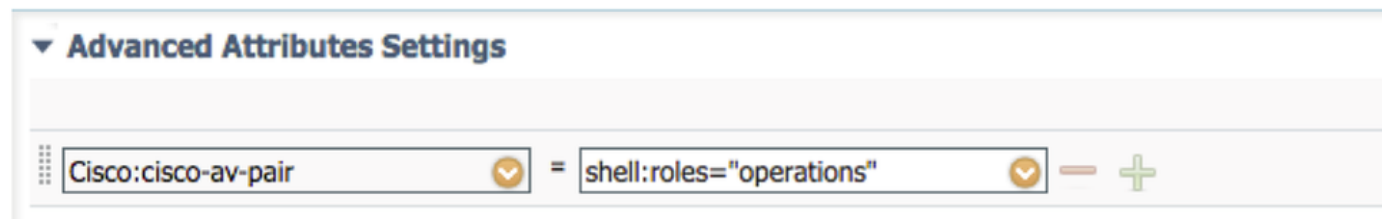
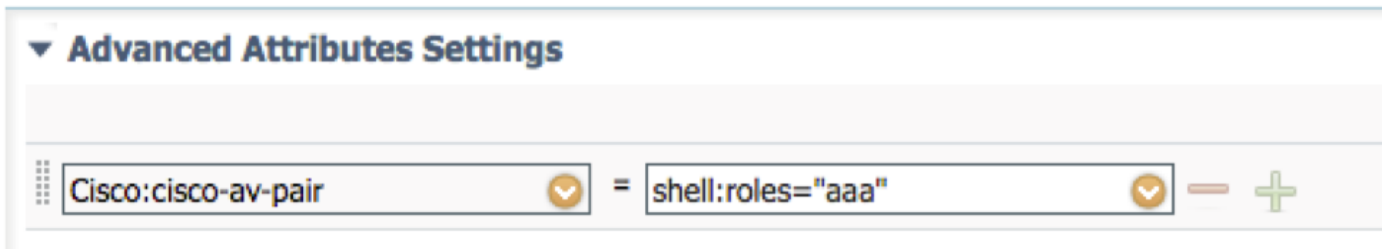


步驟3. 使用以下Cisco-AV配對對其餘使用者角色重複步驟2

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

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

cisco-av-pair=shell:roles="只讀"



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

Authentication Authorization Profiling Posture Client Provisioning > Policy Elements

Dictionarys > Conditions > Results

### Standard Authorization Profiles

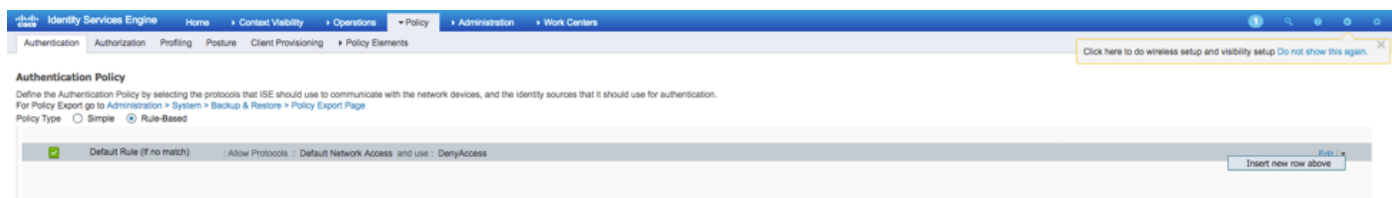
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Edit + Add Duplicate Delete

<input type="checkbox"/>	Name	Profile
<input type="checkbox"/>	Blackhole_Wireless_Access	Cisco ⊕
<input type="checkbox"/>	Cisco_IP_Phones	Cisco ⊕
<input type="checkbox"/>	Cisco_WebAuth	Cisco ⊕
<input type="checkbox"/>	FXOS-AAA-PROFILE	Cisco ⊕
<input type="checkbox"/>	FXOS-ADMIN-PROFILE	Cisco ⊕
<input type="checkbox"/>	FXOS-OPER-PROFILE	Cisco ⊕
<input type="checkbox"/>	FXOS-ReadOnly-PROFILE	Cisco ⊕

建立身份驗證策略

步驟1. 導覽至Policy > Authentication > , 然後點選要建立規則的位置旁邊的箭頭。



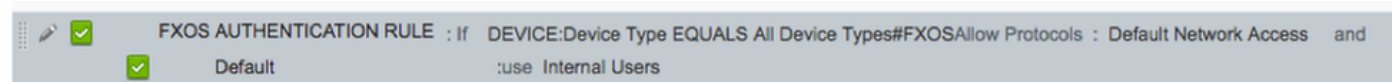
步驟2. 設定簡單；可以更精細地完成，但在本範例中，我們將使用裝置型別：

名稱:FXOS驗證規則

IF選擇新屬性/值：裝置：裝置型別等於所有裝置型別#FXOS

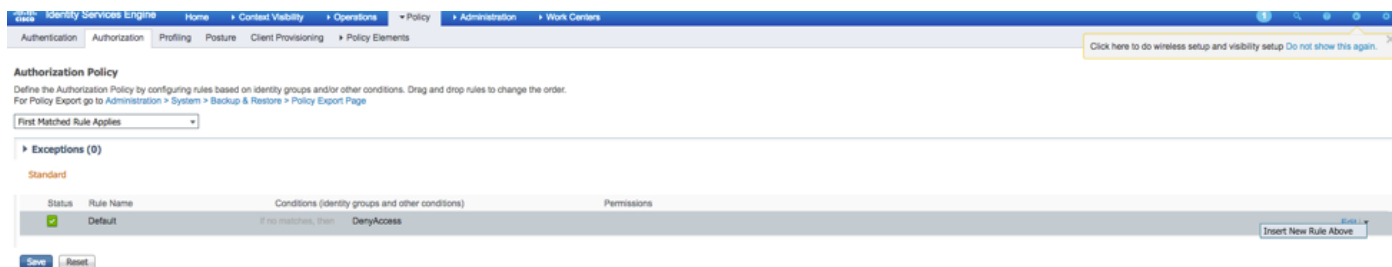
允許協定：預設網路訪問

使用:內部使用者



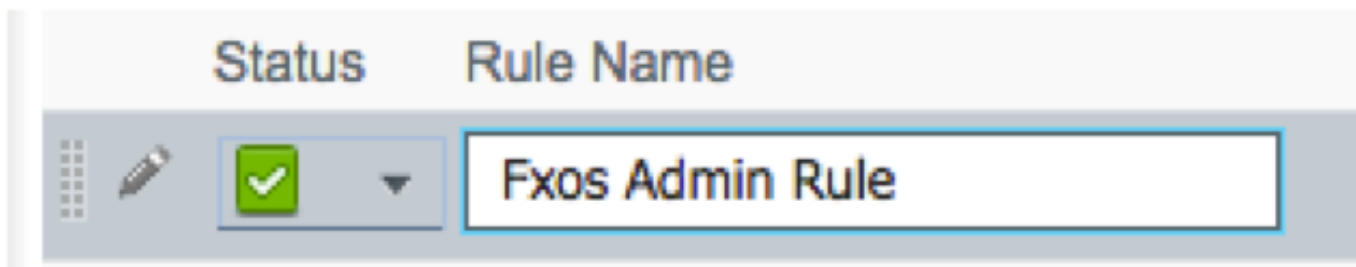
## 建立授權策略

步驟1. 導覽至Policy > Authorization > , 然後點選箭頭網以編輯您要建立規則的位置。

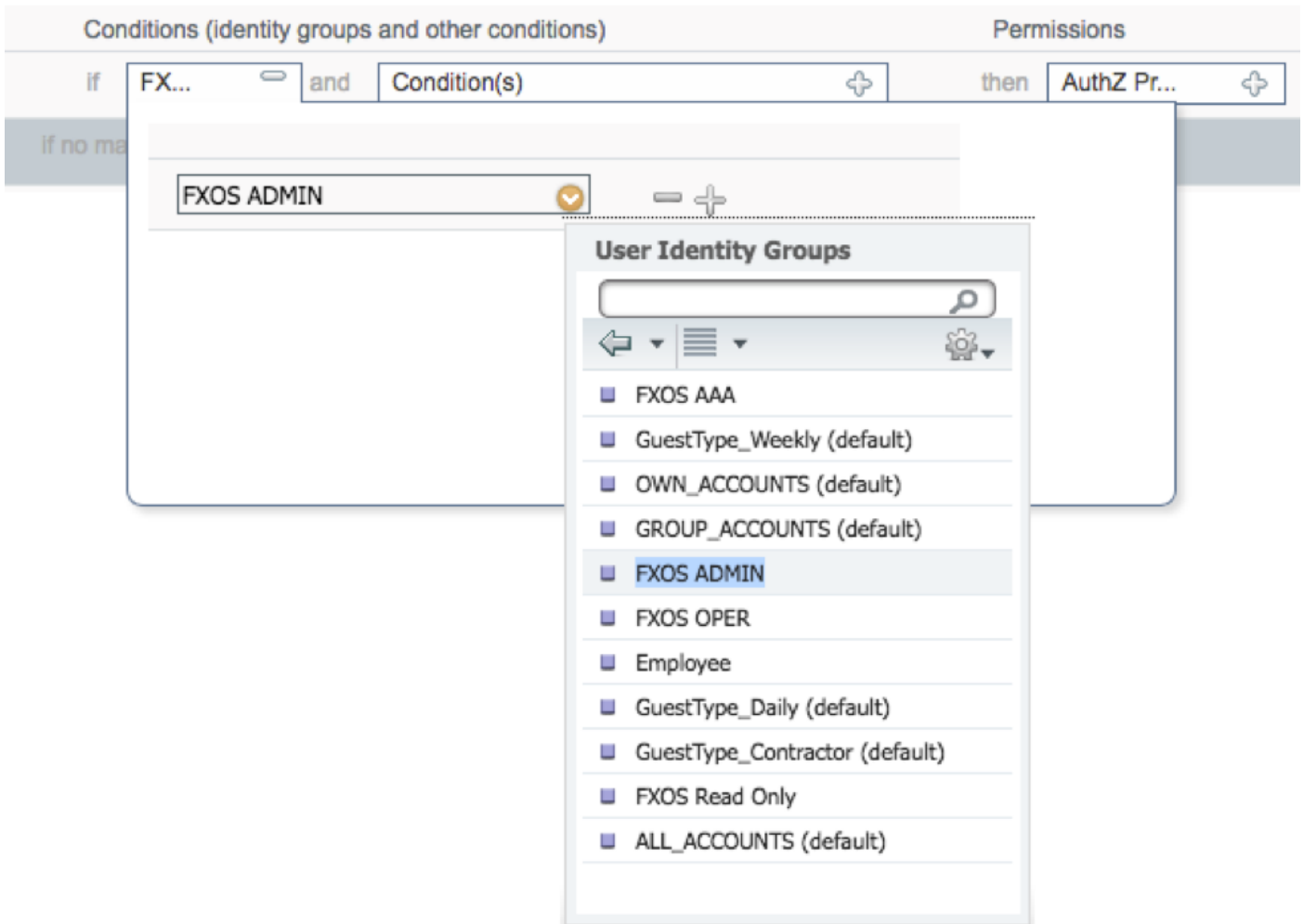


步驟2. 使用所需引數輸入授權規則的值。

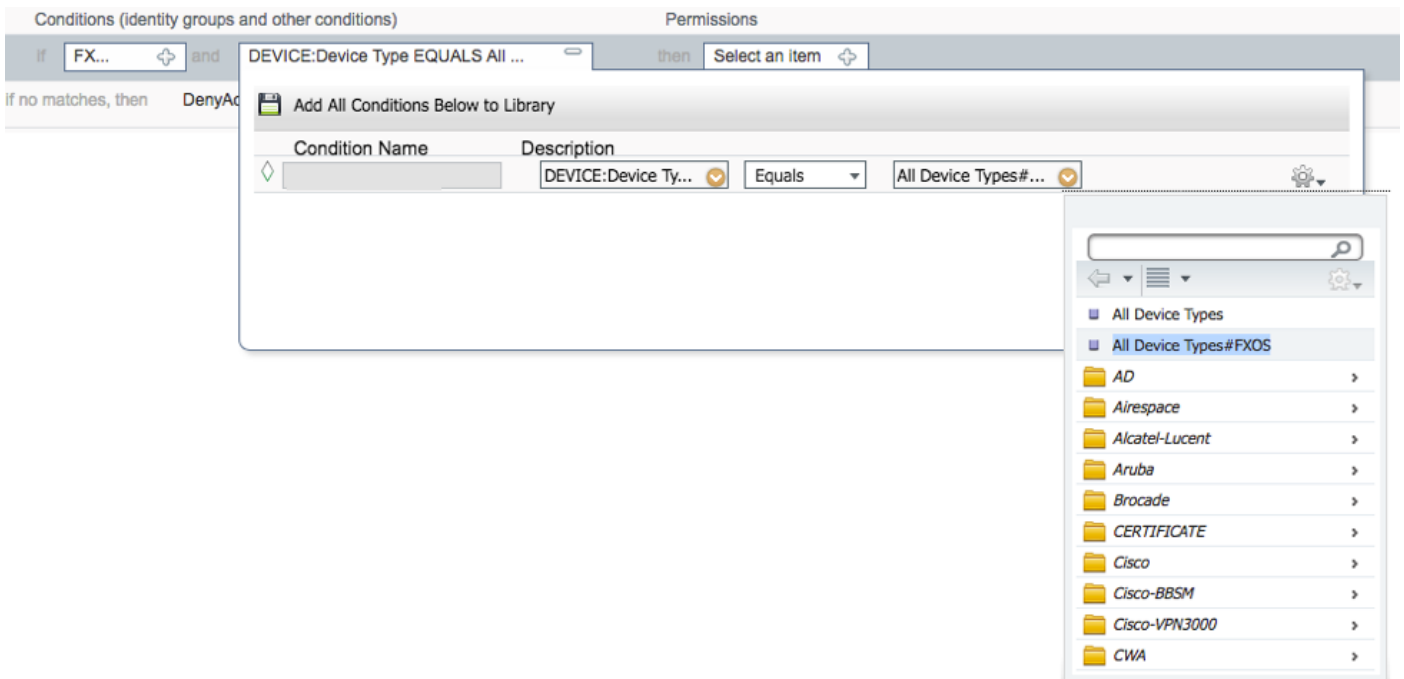
2.1. 規則名稱：Fxs <USER ROLE>規則。



2.2. 如果：使用者身份組>選擇<使用者角色>。



2.3.和 : Create New Condition > Device:Device type Equals All Devices Types #FXOS。



2.4.許可權 : 標準>選擇使用者角色配置檔案

Permissions

then FXOS-A...

FXOS-ADMIN-PROFILE

**Standard**

Blackhole\_Wireless\_Access

Cisco\_IP\_Phones

Cisco\_WebAuth

DenyAccess

FXOS-AAA-PROFILE

**FXOS-ADMIN-PROFILE**

FXOS-OPER-PROFILE

FXOS-ReadOnly-PROFILE

NSP\_Onboard

Non\_Cisco\_IP\_Phones

PermitAccess

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Fxos Admin Rule	if <b>FXOS ADMIN</b> AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ADMIN-PROFILE

步驟3.對所有使用者角色重複步驟2。

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Fxos Admin Rule	if <b>FXOS ADMIN</b> AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ADMIN-PROFILE
<input checked="" type="checkbox"/>	Fxos AAA Rule	if <b>FXOS AAA</b> AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-AAA-PROFILE
<input checked="" type="checkbox"/>	Fxos Oper Rule	if <b>FXOS OPER</b> AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-OPER-PROFILE
<input checked="" type="checkbox"/>	Fxos Read only Rule	if <b>FXOS Read Only</b> AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ReadOnly-PROFILE
<input checked="" type="checkbox"/>	Default	if no matches, then DenyAccess	

步驟4.按一下頁面底部的Save。

 Save Reset

## 驗證

現在，您可以測試每個使用者並驗證分配的使用者角色。

### FXOS機箱驗證

1. 通過Telnet或SSH連線到FXOS機箱，並使用ISE上任何建立的使用者登入。

使用者名稱:fxosadmin

密碼：

fpr4120-TAC-A#scope**安全**

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

遠端使用者**fxosaa**:

說明:

使用者角色：

名稱:**aaa**

名稱:**唯讀**

遠端使用者**fxosadmin**:

說明:

使用者角色：

名稱:**admin**

名稱:**唯讀**

遠端使用者**fxosper**:

說明:

使用者角色：

名稱:**操作**

名稱:唯讀

遠端使用者fxosro:

說明:

使用者角色 :

名稱:唯讀

根據輸入的使用者名稱，FXOS機箱cli將僅顯示已分配使用者角色的授權命令。

管理員使用者角色。

fpr4120-TAC-A /security # ?

確認確認

clear-user-sessions Clear User Sessions

建立建立託管對象

刪除刪除託管對象

禁用禁用服務

啟用啟用服務

輸入輸入託管對象

作用域更改當前模式

set Set屬性值

顯示顯示系統資訊

終止活動的cimc會話

fpr4120-TAC-A#connect fxos

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

fpr4120-TAC-A(fxos)#

只讀使用者角色。

fpr4120-TAC-A /security # ?

作用域更改當前模式

set Set屬性值

顯示顯示系統資訊

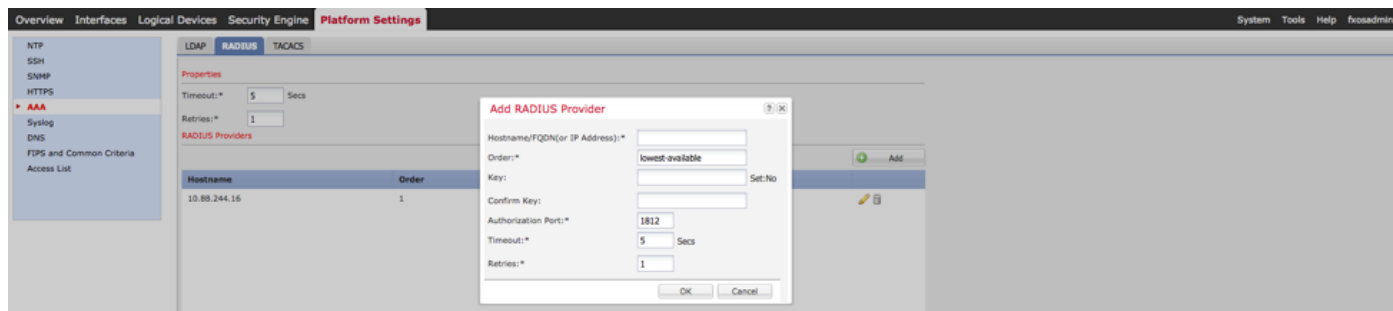


fxpr4120-TAC-A#connect fxos

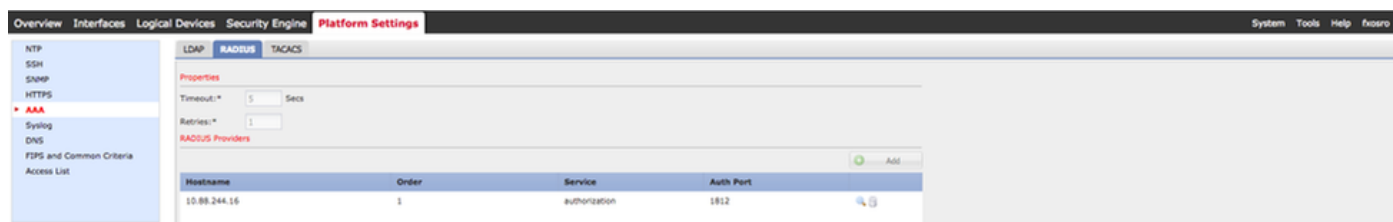
fxpr4120-TAC-A(fxos)# debug aaa aaa-requests

%角色許可權被拒絕

2. 瀏覽至FXOS機箱IP地址並使用ISE上任何建立的使用者登入。  
管理員使用者角色。



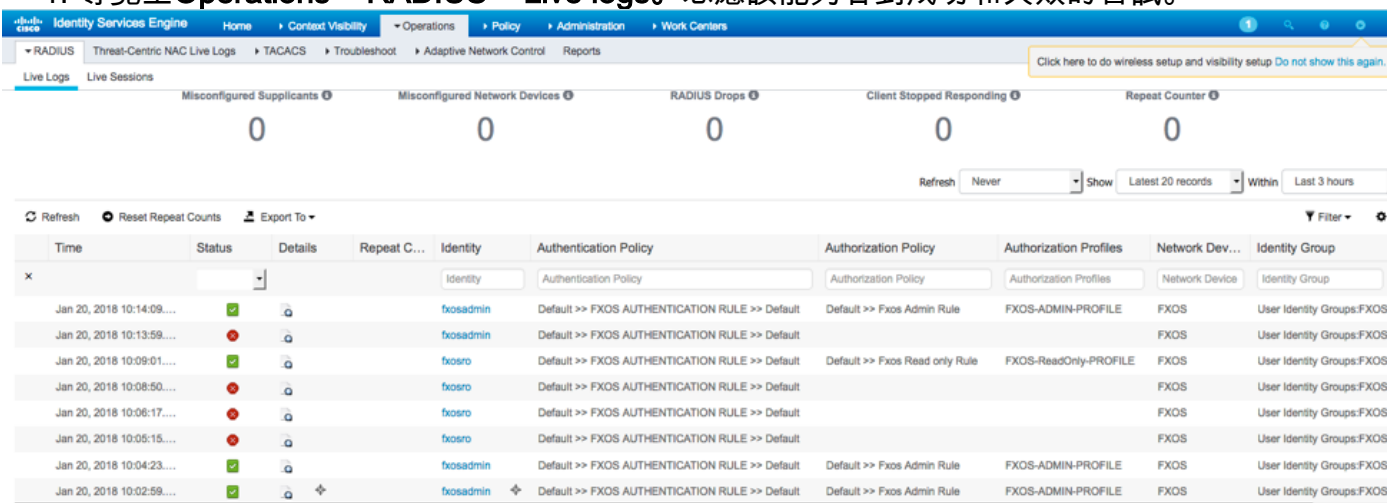
只讀使用者角色。



附註：請注意，ADD按鈕呈灰色顯示。

## ISE 2.0驗證

1. 導覽至Operations > RADIUS > Live logs。您應該能夠看到成功和失敗的嘗試。



## 疑難排解

為了調試AAA身份驗證和授權，請在FXOS cli中運行以下命令。

fpr4120-TAC-A#connect **fxos**

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

fpr4120-TAC-A(fxos)# **debug aaa event**

fpr4120-TAC-A(fxos)# **debug aaa errors**

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

成功嘗試身份驗證後，您將看到以下輸出。

2018年1月20日17:18:02.410275 aaa:用於身份驗證的aaa\_req\_process。會話編號0

2018年1月20日17:18:02.410297 aaa:aaa\_req\_process:來自裝置的常規AAA請求：login  
appn\_subtype:預設

2018年1月20日17:18:02.410310 aaa:try\_next\_aaa\_method

2018年1月20日17:18:02.410330 aaa:配置的方法總數為1，要嘗試的當前索引為0

2018年1月20日17:18:02.410344 aaa:handle\_req\_using\_method

2018年1月20日17:18:02.410356 aaa:AAA\_METHOD\_SERVER\_GROUP

2018年1月20日17:18:02.410367 aaa:aaa\_sg\_method\_handler group = radius

2018年1月20日17:18:02.410379 aaa:使用傳遞到此函式的sg\_protocol

2018年1月20日17:18:02.410393 aaa:正在向RADIUS服務傳送請求

2018年1月20日17:18:02.412944 aaa:mts\_send\_msg\_to\_prot\_daemon:負載長度= 374

2018年1月20日17:18:02.412973 aaa:會話：0x8dfd68c已新增到會話表1

2018年1月20日17:18:02.412987 aaa:配置的方法組成功

2018年1月20日17:18:02.656425 aaa:aaa\_process\_fd\_set

2018年1月20日17:18:02.656447 aaa:aaa\_process\_fd\_set:aaa\_q上的mtscallback

2018年1月20日17:18:02.656470 aaa:mts\_message\_response\_handler:mts響應

2018年1月20日17:18:02.656483 aaa:prot\_daemon\_response\_handler

2018年1月20日17:18:02.656497 aaa:會話：0x8dfd68c已從會話表0中刪除

2018年1月20日17:18:02.656512 aaa:is\_aaa\_resp\_status\_success status = 1

2018年1月20日17:18:02.656525 aaa:is\_aaa\_resp\_status\_success為TRUE

2018年1月20日17:18:02.656538 aaa:用於身份驗證的aaa\_send\_client\_response。session->flags=21. aaa\_resp->flags=0。

2018年1月20日17:18:02.656550 aaa:AAA\_REQ\_FLAG\_NORMAL

2018年1月20日17:18:02.656577 aaa:mts\_send\_response成功

2018年1月20日17:18:02.700520 aaa:aaa\_process\_fd\_set:aaa\_accounting\_q上的mtscallback

2018年1月20日17:18:02.700688 aaa:舊操作碼 : accounting\_interim\_update

2018年1月20日17:18:02.700702 aaa:aaa\_create\_local\_acct\_req:user=, session\_id=, log=added user fxosro

2018年1月20日17:18:02.700725 aaa:aaa\_req\_process用於記帳。 會話編號0

2018年1月20日17:18:02.700738 aaa:MTS請求引用為空。 LOCAL請求

2018年1月20日17:18:02.700749 aaa:設定AAA\_REQ\_RESPONSE\_NOT\_NEEDED

2018年1月20日17:18:02.700762 aaa:aaa\_req\_process:來自裝置的常規AAA請求 : default appln\_subtype:預設

2018年1月20日17:18:02.700774 aaa:try\_next\_aaa\_method

2018年1月20日17:18:02.700798 aaa:沒有針對預設預設配置的方法

2018年1月20日17:18:02.700810 aaa:沒有可用於此請求的配置

2018年1月20日17:18:02.700997 aaa:aaa\_send\_client\_response用於記帳。 session->flags=254. aaa\_resp->flags=0。

2018年1月20日17:18:02.701010 aaa:舊庫記帳請求的響應將作為SUCCESS傳送

2018年1月20日17:18:02.701021 aaa:此請求不需要響應

2018年1月20日17:18:02.701033 aaa:AAA\_REQ\_FLAG\_LOCAL\_RESP

2018年1月20日17:18:02.701044 aaa:aaa\_cleanup\_session

2018年1月20日17:18:02.701055 aaa:應釋放aaa\_req。

2018年1月20日17:18:02.701067 aaa:回退方法本地成功

2018年1月20日17:18:02.706922 aaa:aaa\_process\_fd\_set

2018年1月20日17:18:02.706937 aaa:aaa\_process\_fd\_set:aaa\_accounting\_q上的mtscallback

2018年1月20日17:18:02.706959 aaa:舊操作碼 : accounting\_interim\_update

2018年1月20日17:18:02.706972 aaa:aaa\_create\_local\_acct\_req:user=, session\_id=, log=added user:fxosr to the role:read-only

身份驗證嘗試失敗後，您將看到以下輸出。

2018年1月20日17:15:18.102130 aaa:aaa\_process\_fd\_set

2018年1月20日17:15:18.102149 aaa:aaa\_process\_fd\_set:aaa\_q上的mtscallback

2018年1月20日17:15:18.102267 aaa:aaa\_process\_fd\_set

2018年1月20日17:15:18.102281 aaa:aaa\_process\_fd\_set:aaa\_q上的mtscallback

2018年1月20日17:15:18.102363 aaa:aaa\_process\_fd\_set

2018年1月20日17:15:18.102377 aaa:aaa\_process\_fd\_set:aaa\_q上的mtscallback

2018年1月20日17:15:18.102456 aaa:aaa\_process\_fd\_set

2018年1月20日17:15:18.102468 aaa:aaa\_process\_fd\_set:aaa\_q上的mtscallback

2018年1月20日17:15:18.102489 aaa:mts\_aaa\_req\_process

2018年1月20日17:15:18.102503 aaa:用於身份驗證的aaa\_req\_process。會話編號0

2018年1月20日17:15:18.102526 aaa:aaa\_req\_process:來自裝置的常規AAA請求 : login  
appn\_subtype:預設

2018年1月20日17:15:18.102540 aaa:try\_next\_aaa\_method

2018年1月20日17:15:18.102562 aaa:配置的方法總數為1 , 要嘗試的當前索引為0

2018年1月20日17:15:18.102575 aaa:handle\_req\_using\_method

2018年1月20日17:15:18.102586 aaa:AAA\_METHOD\_SERVER\_GROUP

2018年1月20日17:15:18.102598 aaa:aaa\_sg\_method\_handler group = radius

2018年1月20日17:15:18.102610 aaa:使用傳遞到此函式的sg\_protocol

2018年1月20日17:15:18.102625 aaa:正在向RADIUS服務傳送請求

2018年1月20日17:15:18.102658 aaa:mts\_send\_msg\_to\_prot\_daemon:負載長度= 371

2018年1月20日17:15:18.102684 aaa:會話 : 0x8dfd68c已新增到會話表1

2018年1月20日17:15:18.102698 aaa:配置的方法組成功

2018年1月20日17:15:18.273682 aaa:aaa\_process\_fd\_set

2018年1月20日17:15:18.273724 aaa:aaa\_process\_fd\_set:aaa\_q上的mtscallback

2018年1月20日17:15:18.273753 aaa:mts\_message\_response\_handler:mts響應

2018年1月20日17:15:18.273768 aaa:prot\_daemon\_response\_handler

2018年1月20日17:15:18.273783 aaa:會話 : 0x8dfd68c已從會話表0中刪除

2018年1月20日17:15:18.273801 aaa:is\_aaa\_resp\_status\_success status = 2

2018年1月20日17:15:18.273815 aaa:is\_aaa\_resp\_status\_success為TRUE

2018年1月20日17:15:18.273829 aaa:用於身份驗證的aaa\_send\_client\_response。session->flags=21. aaa\_resp->flags=0。

2018年1月20日17:15:18.273843 aaa:AAA\_REQ\_FLAG\_NORMAL

2018年1月20日17:15:18.273877 aaa:mts\_send\_response成功

2018年1月20日17:15:18.273902 aaa:aaa\_cleanup\_session

2018年1月20日17:15:18.273916 aaa:請求消息的mts\_drop

2018年1月20日17:15:18.273935 aaa:應釋放aaa\_req。

2018年1月20日17:15:18.280416 aaa:aaa\_process\_fd\_set

2018年1月20日17:15:18.280443 aaa:aaa\_process\_fd\_set:aaa\_q上的mtscallback

2018年1月20日17:15:18.280454 aaa:aaa\_enable\_info\_config:GET\_REQ for aaa登入錯誤消息

2018年1月20日17:15:18.280460 aaa:已取回配置操作的返回值：未知安全項

## 相關資訊

啟用TACACS/RADIUS身份驗證後，FX-OS cli上的Ethalyzer命令將提示密碼輸入密碼。此行為是由錯誤引起的。

錯誤id:[CSCvg87518](#)