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

目錄

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TACACS+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 — 對系統配置的只讀訪問許可權，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：

fpr4120-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 Remirez、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
- ISE中需要TACACS+裝置管理許可證

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

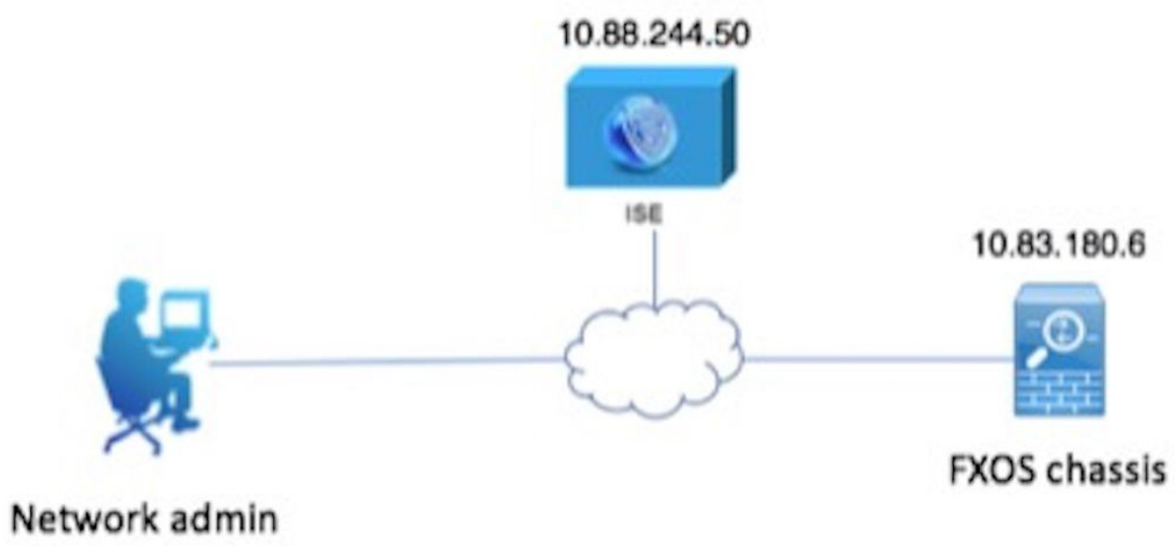
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

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



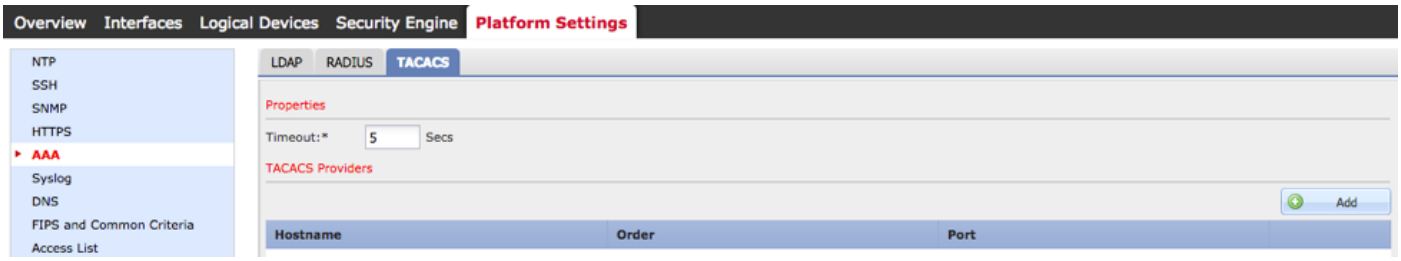
組態

配置FXOS機箱

建立TACACS+提供程式

步驟1.導覽至Platform Settings > AAA。

步驟2.按一下TACACS索引標籤。

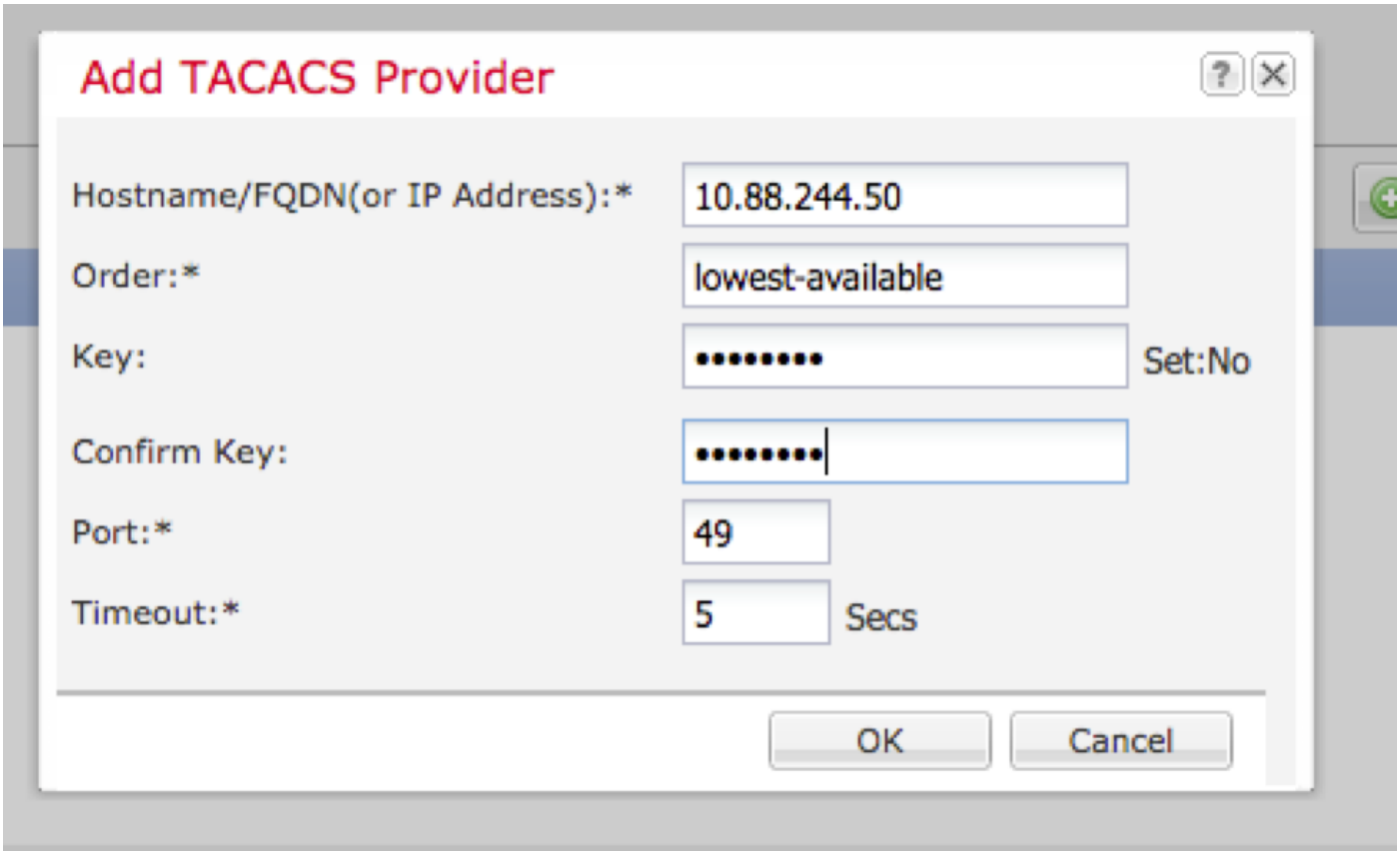


步驟3.對於要新增的每個TACACS+提供程式（最多16個提供程式）。

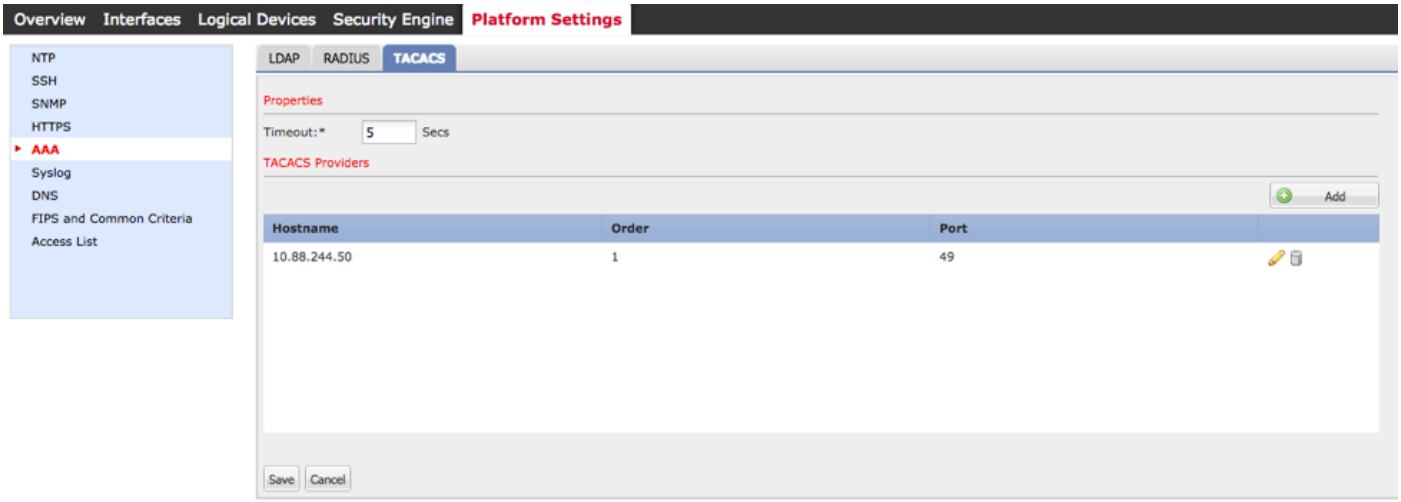
3.1.在TACACS提供程式區域中，按一下Add。

3.2.開啟「新增TACACS提供程式」對話方塊後，輸入所需的值。

3.3.按一下OK關閉「新增TACACS提供程式」對話方塊。

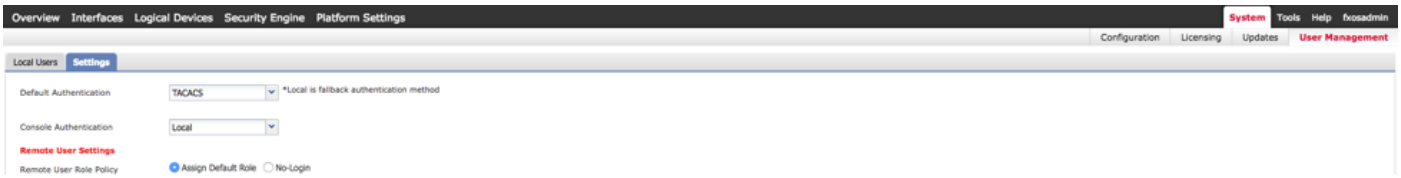


步驟4.按一下「**Save**」。



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

步驟6.在Default Authentication下選擇**TACACS**。



使用CLI建立TACACS+提供程式

步驟1.要啟用TACACS身份驗證，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 tacacs**

步驟2.使用**show detail**命令驗證設定。

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

預設身份驗證：

管理領域：**Tacacs**

操作領域：**Tacacs**

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TACACS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 tacacs**

fpr4120-TAC-A /security/tacacs # **enter server 10.88.244.50**

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

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

輸入金鑰：******

確認金鑰：******

步驟4.使用**show detail**命令驗證設定。

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

TACACS+伺服器：

主機名、FQDN或IP地址：10.88.244.50

描述：

訂購：1

連接埠:49

主要:****

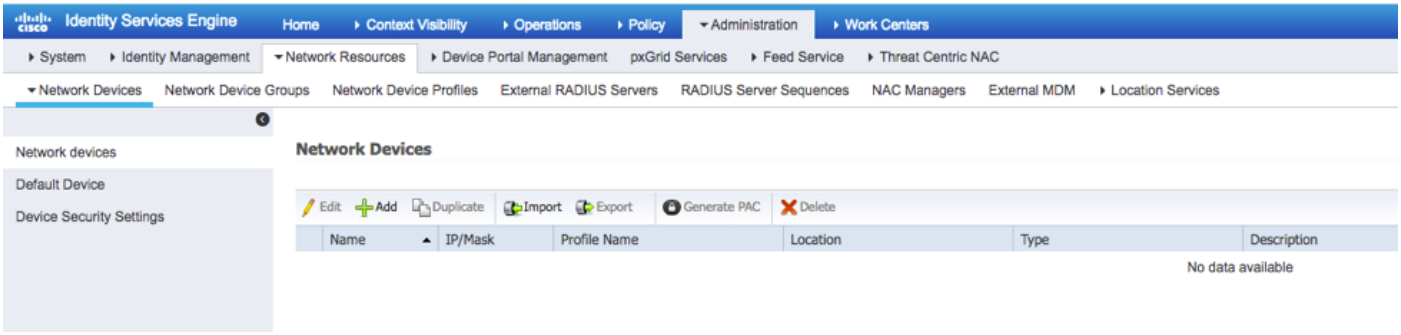
逾時:5

配置ISE伺服器

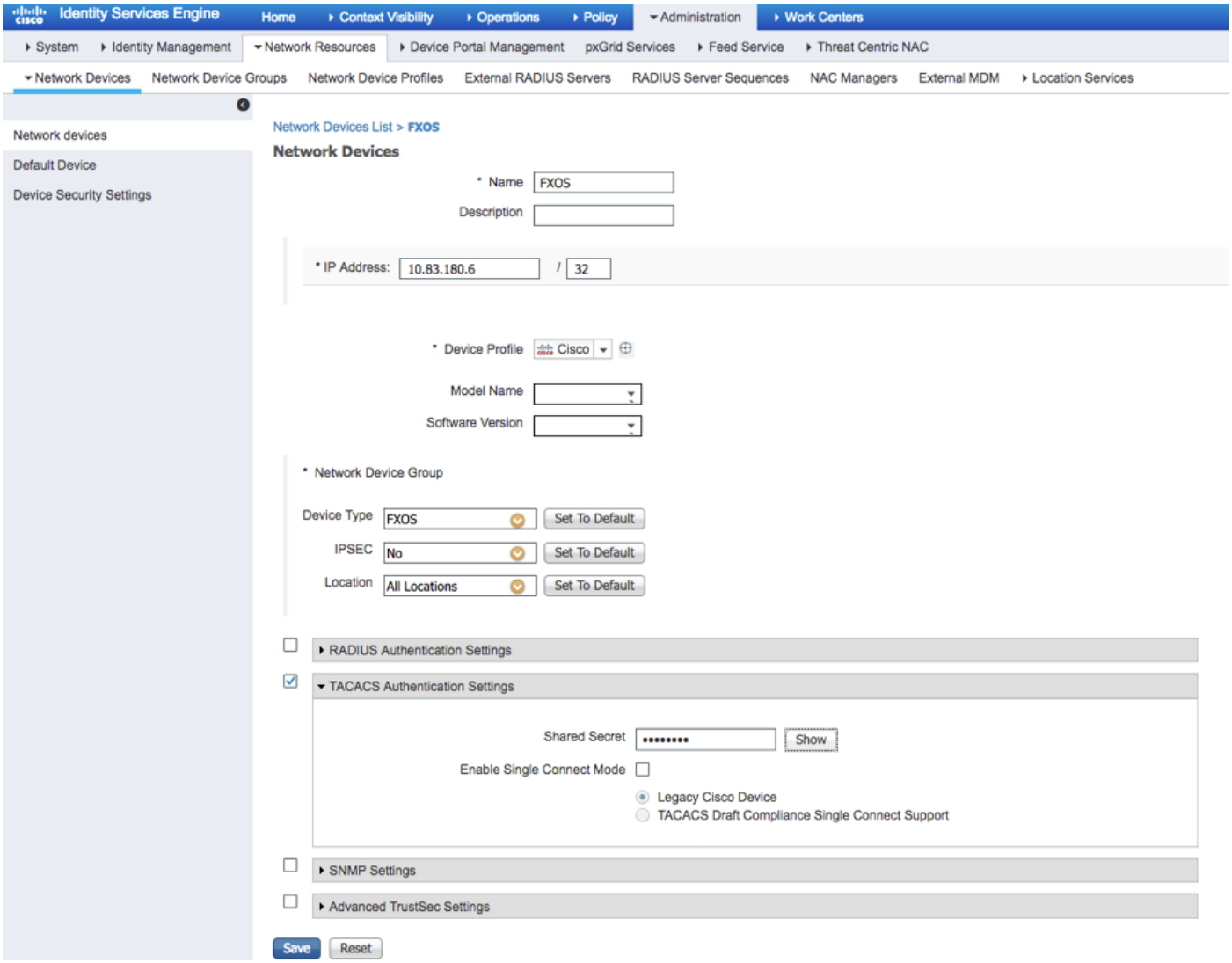
將FXOS新增為網路資源

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

步驟2.按一下**ADD**。



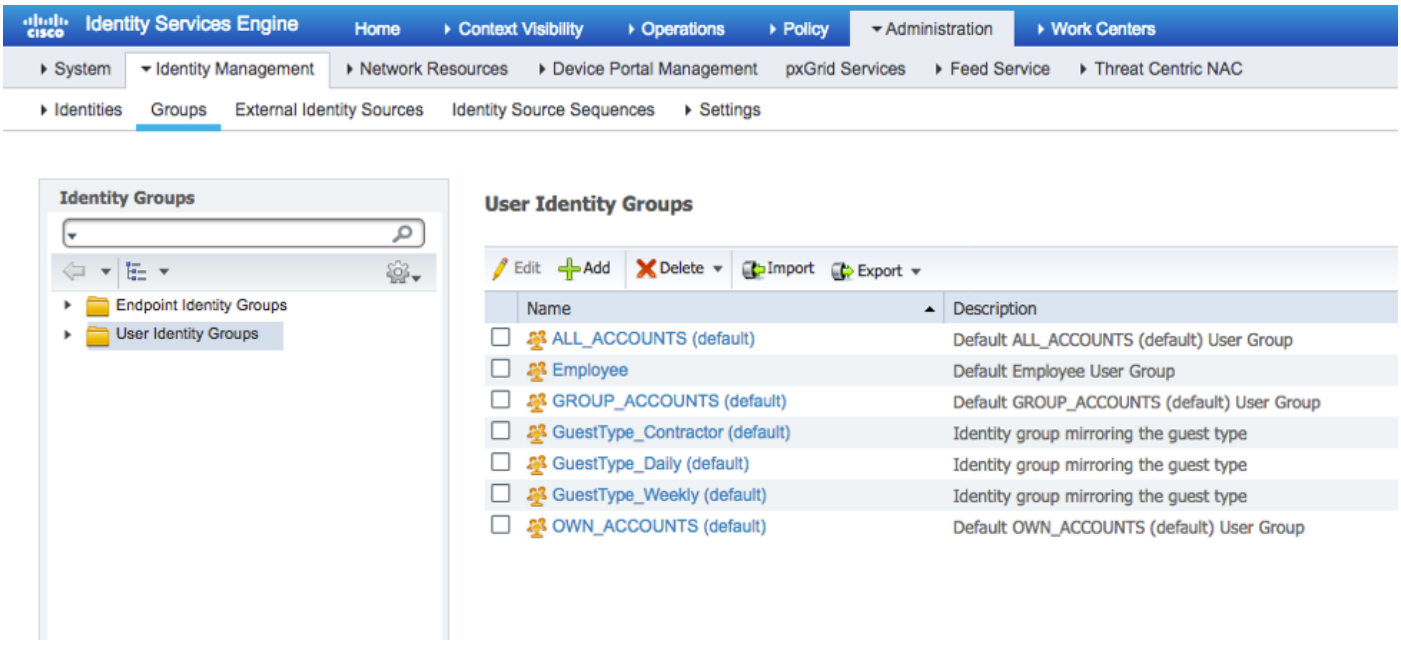
步驟3.輸入所需的值（名稱、IP地址、裝置型別和啟用TACACS+並新增金鑰），然後點選**提交**。



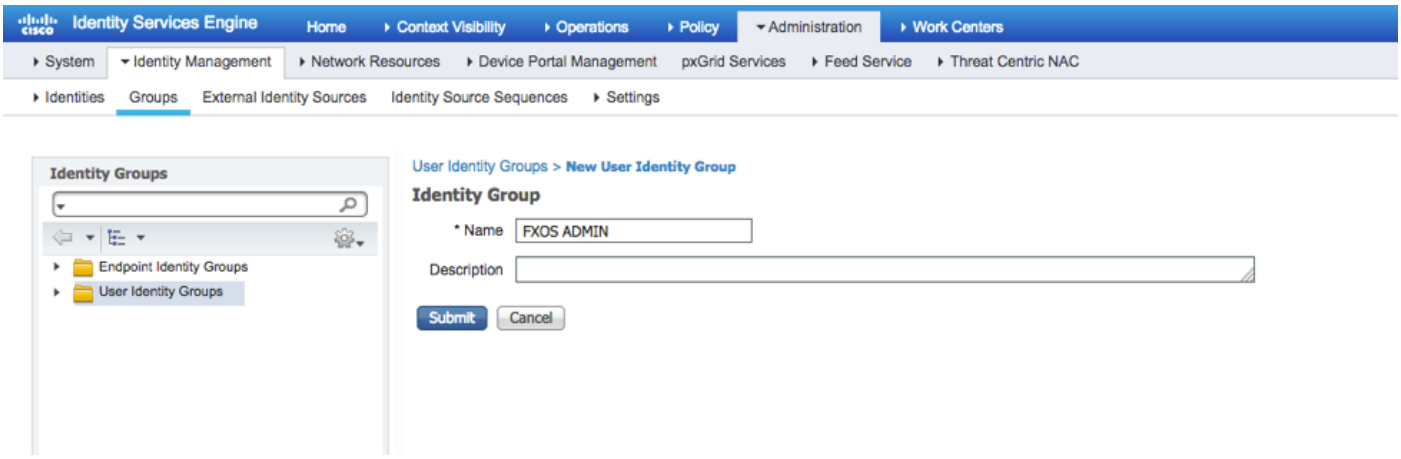
建立身份組和使用者

步驟1.導航到**管理>身份管理>組>使用者身份組。**

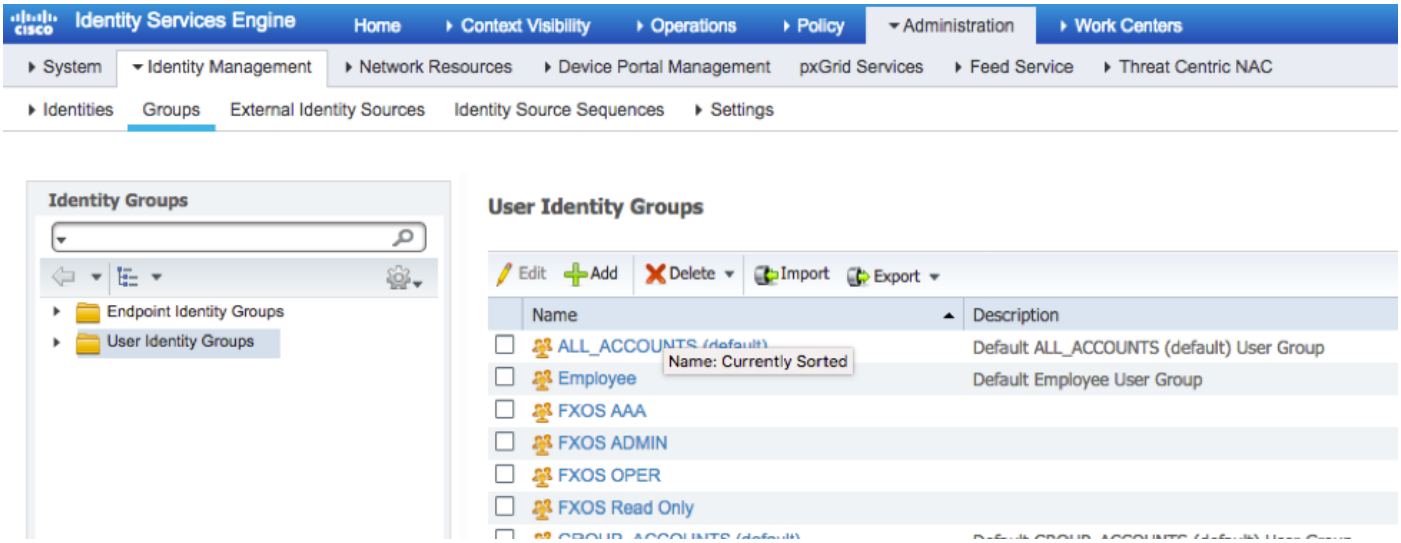
步驟2.按一下**ADD。**



步驟3.輸入Name的值，然後按一下**Submit**。

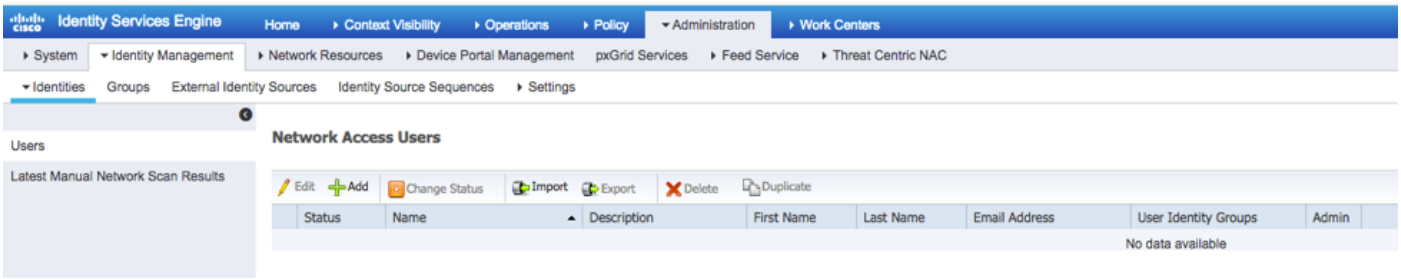


步驟4.對所有所需的使用者角色重複步驟3。

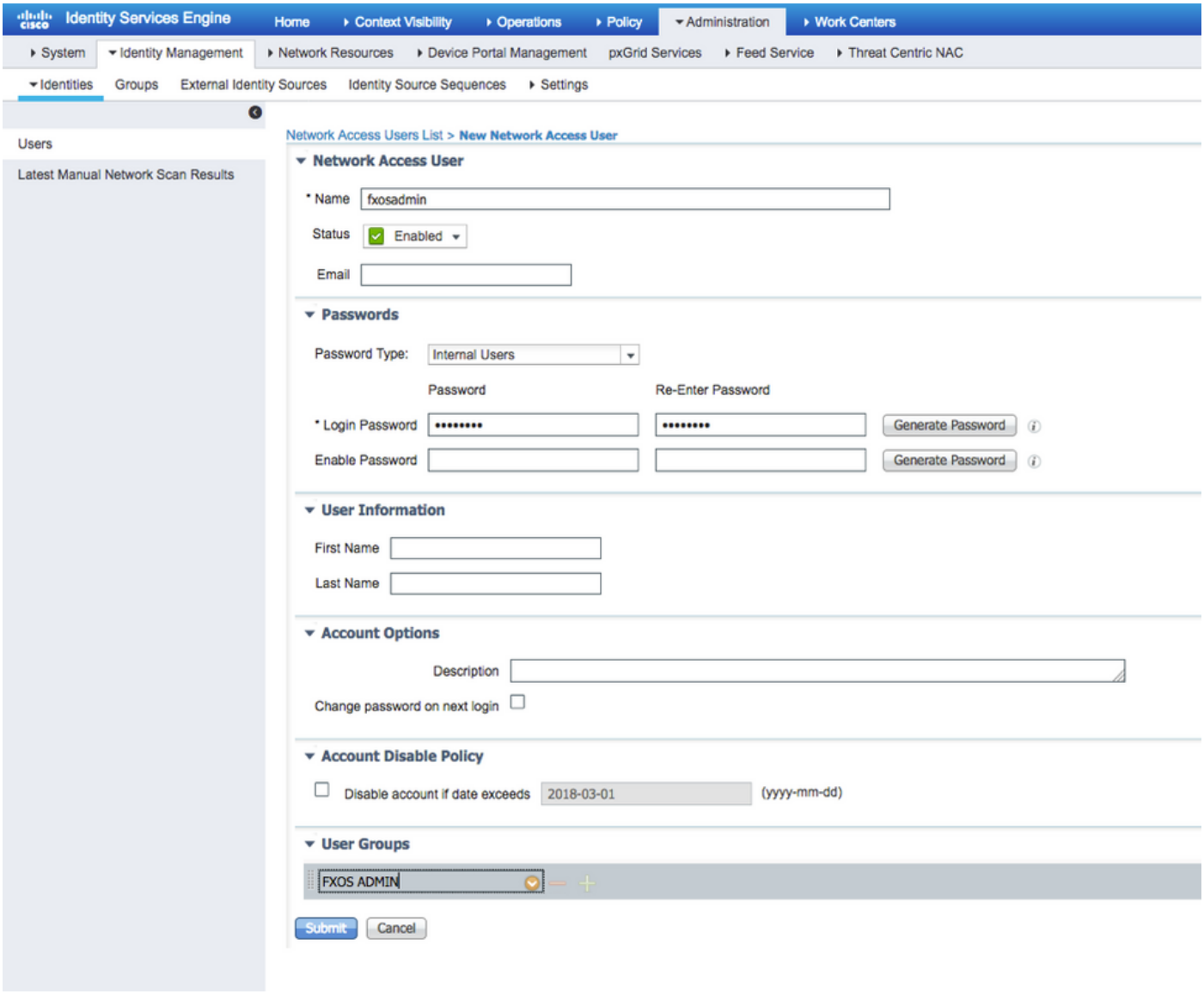


步驟5.導航到**管理>身份管理>身份>使用者**。

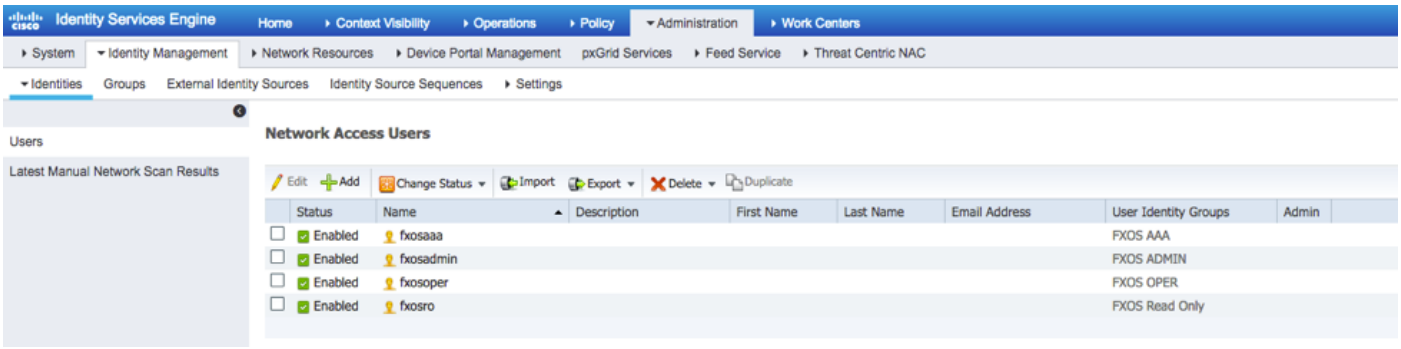
步驟6.按一下**ADD**。



步驟7.輸入所需的值（名稱、使用者組和密碼）。

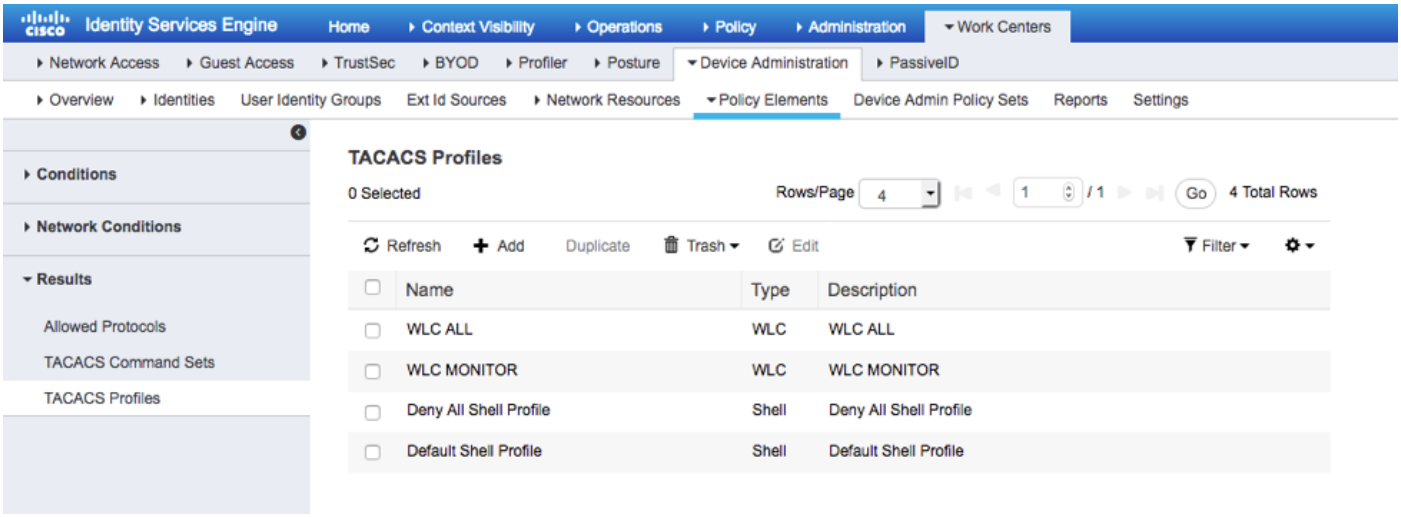


步驟8.對所有必需使用者重複步驟6。



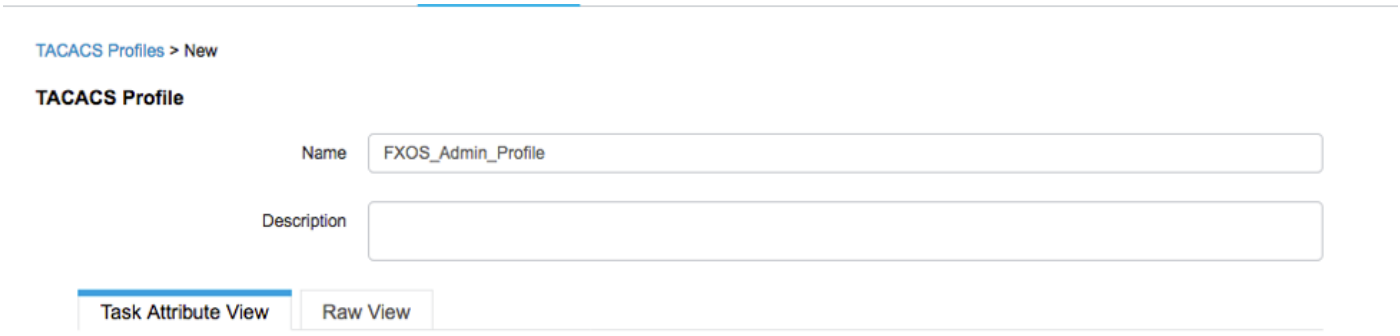
為每個使用者角色建立外殼配置檔案

步驟1。導覽至**工作中心>裝置管理>原則元素>結果> TACACS設定檔**，然後按一下**+ADD**。



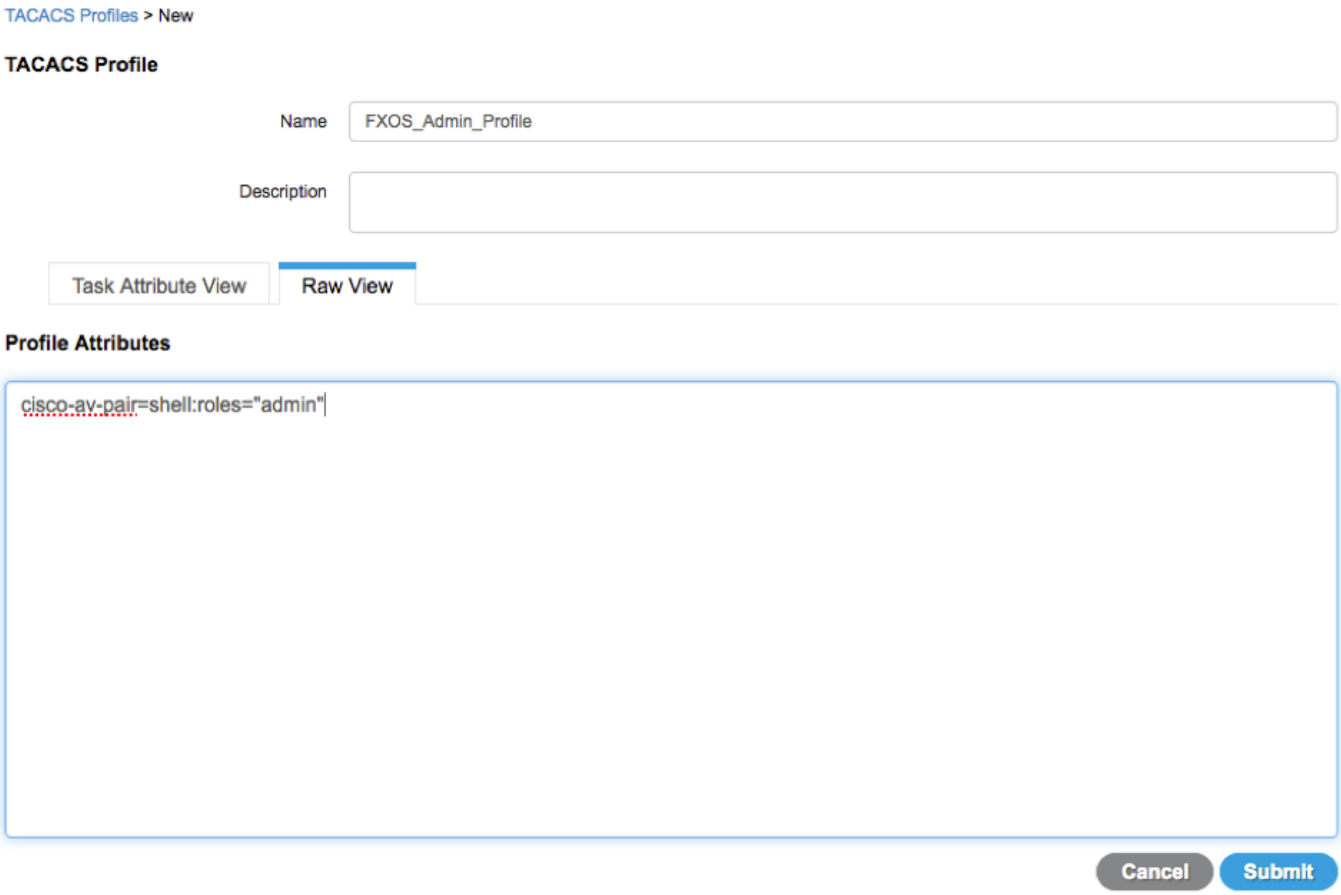
步驟2.輸入TACACS配置檔案所需的值

2.1.輸入名稱。

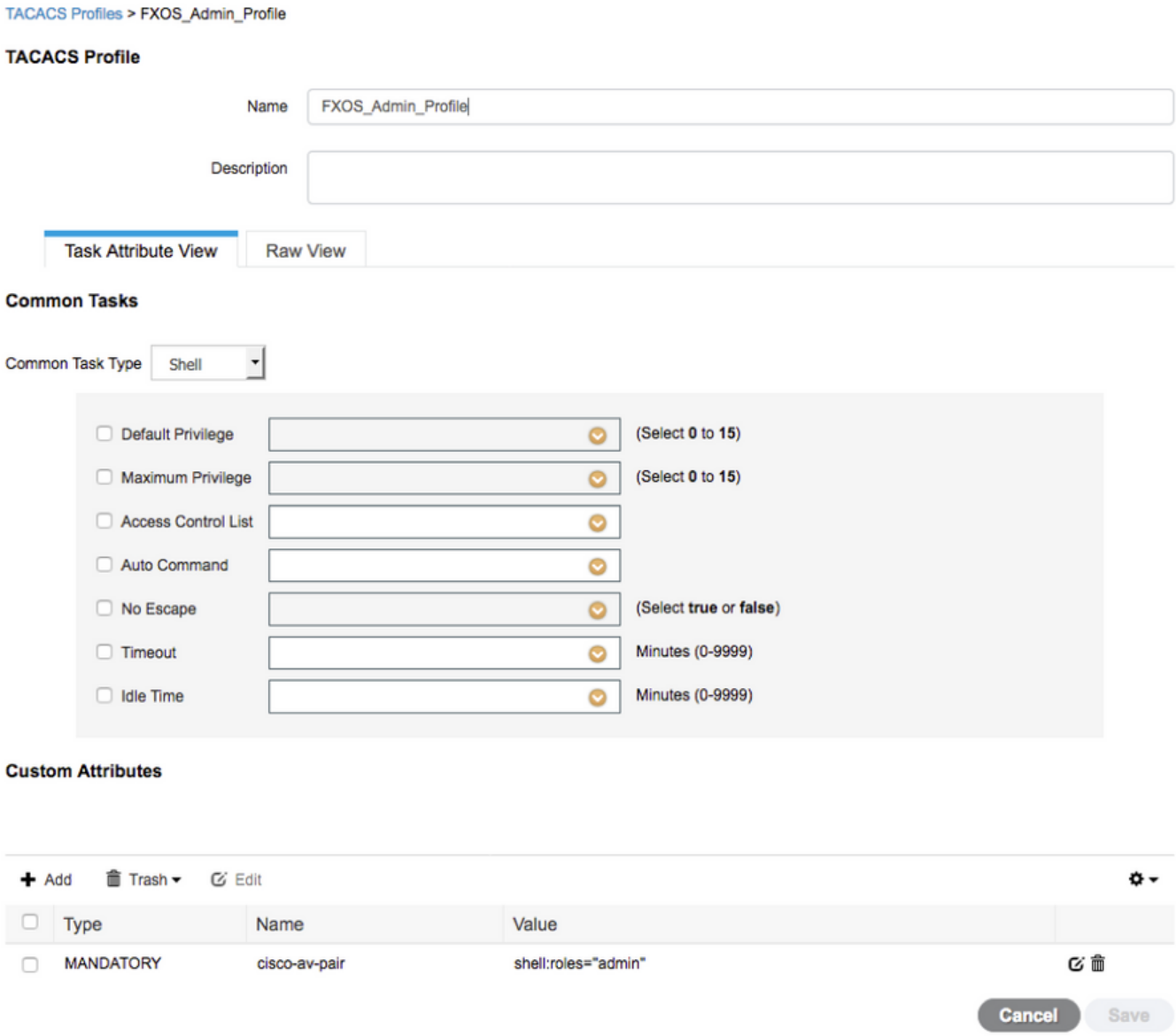


2.2.在**原始檢視**頁籤中，配置以下CISCO-AV配對。

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



2.3.按一下**Submit**。



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"

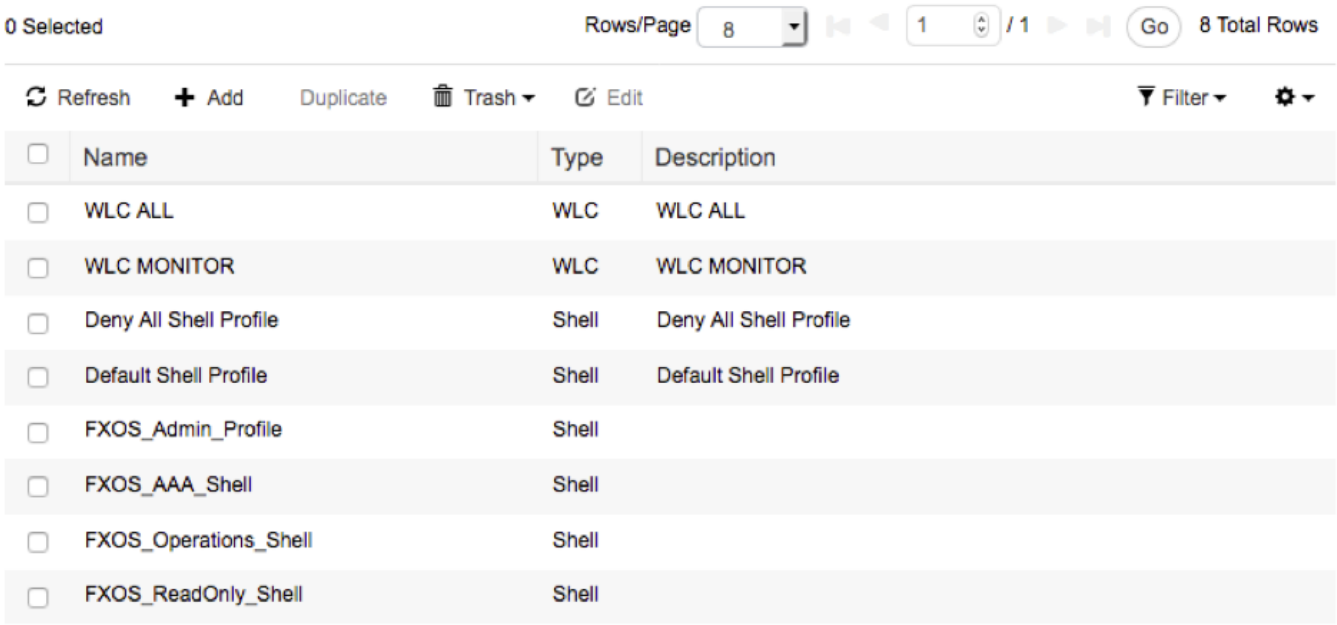
cisco-av-pair=shell:roles="operations"

cisco-av-pair=shell:roles="只讀"

Custom Attributes

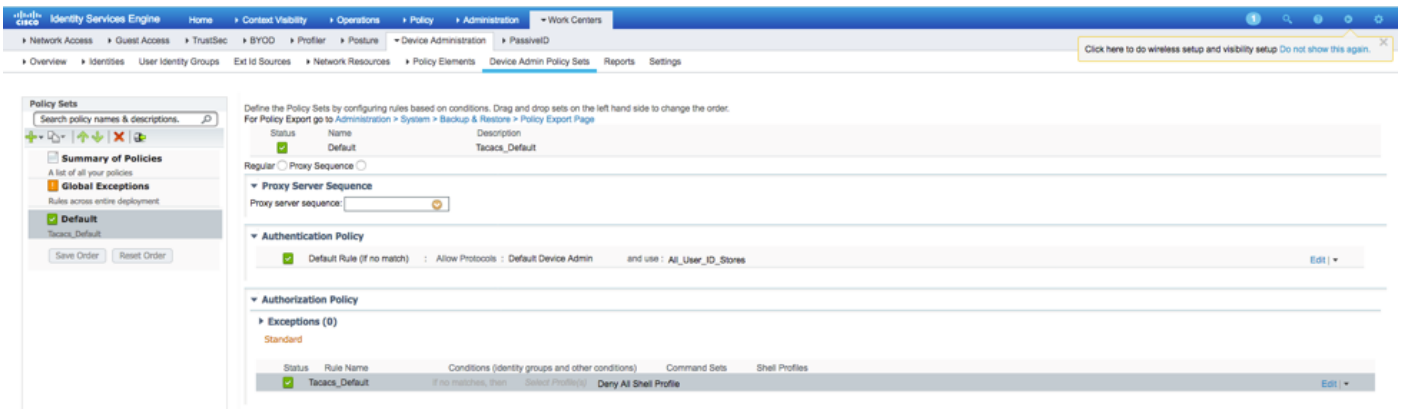
Custom Attributes

TACACS Profiles

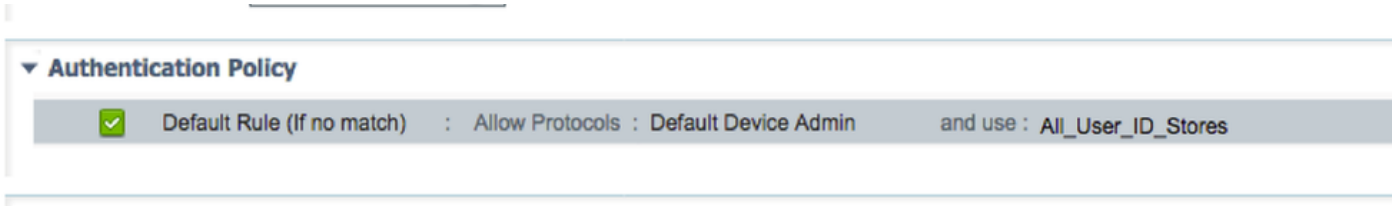


建立TACACS授權策略

步驟1.導航到**工作中心>裝置管理>裝置管理策略集。**



步驟2.確保身份驗證策略指向內部使用者資料庫或所需的身份庫。



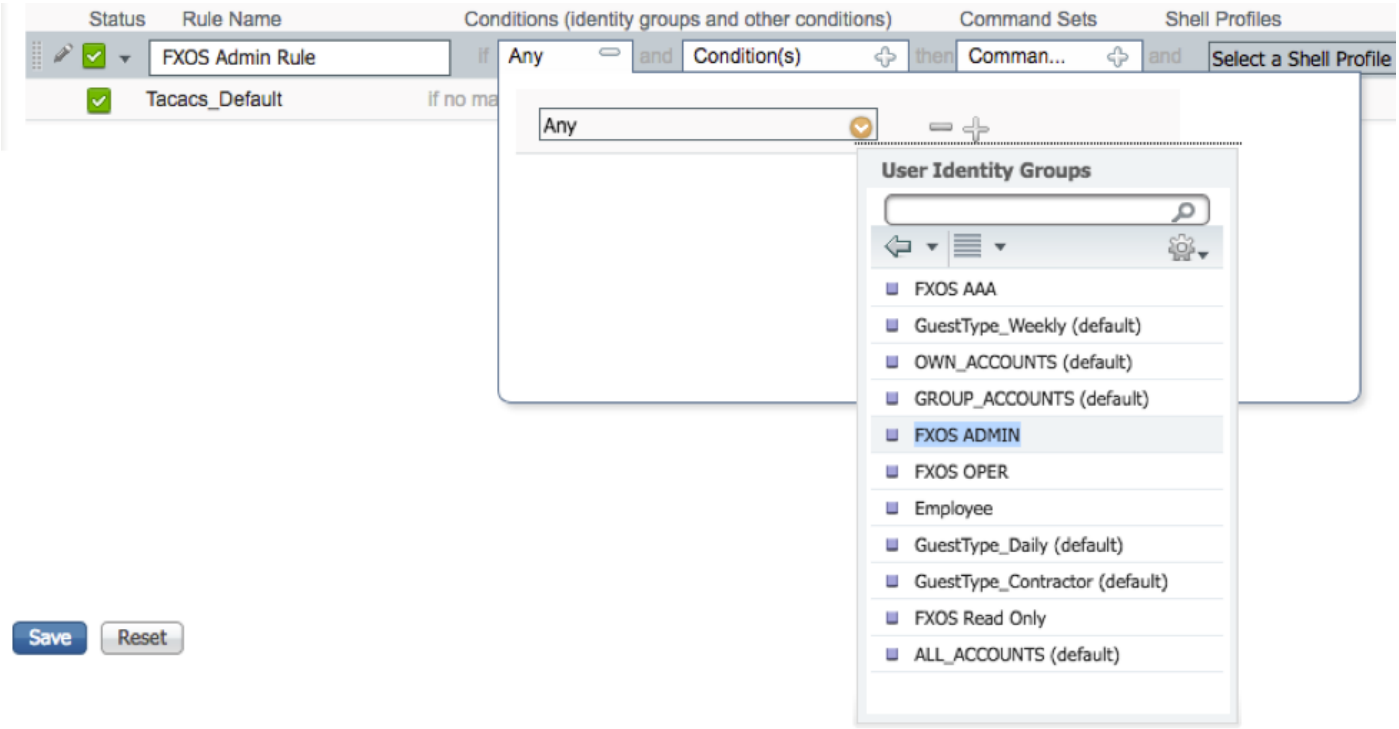
步驟3.按一下預設授權策略末尾的箭頭，然後按一下上面的插入規則。

步驟4.輸入具有所需引數的規則值：

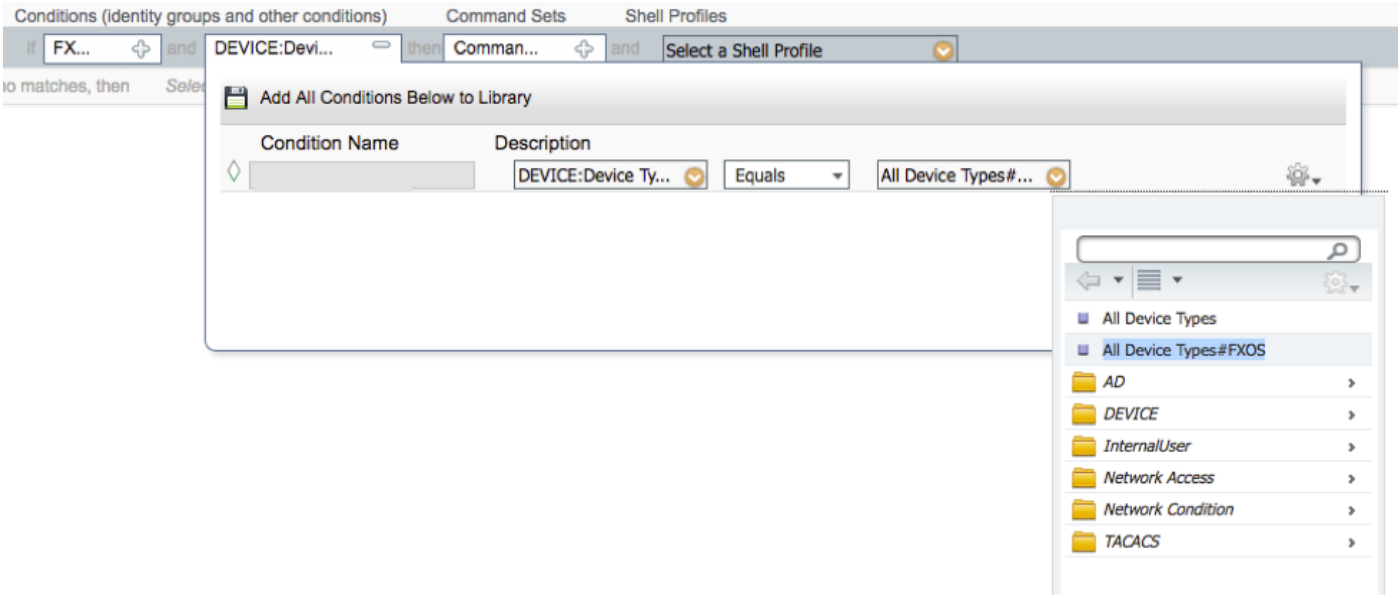
4.1.規則名稱：FXOS管理規則。

4.2.條件。

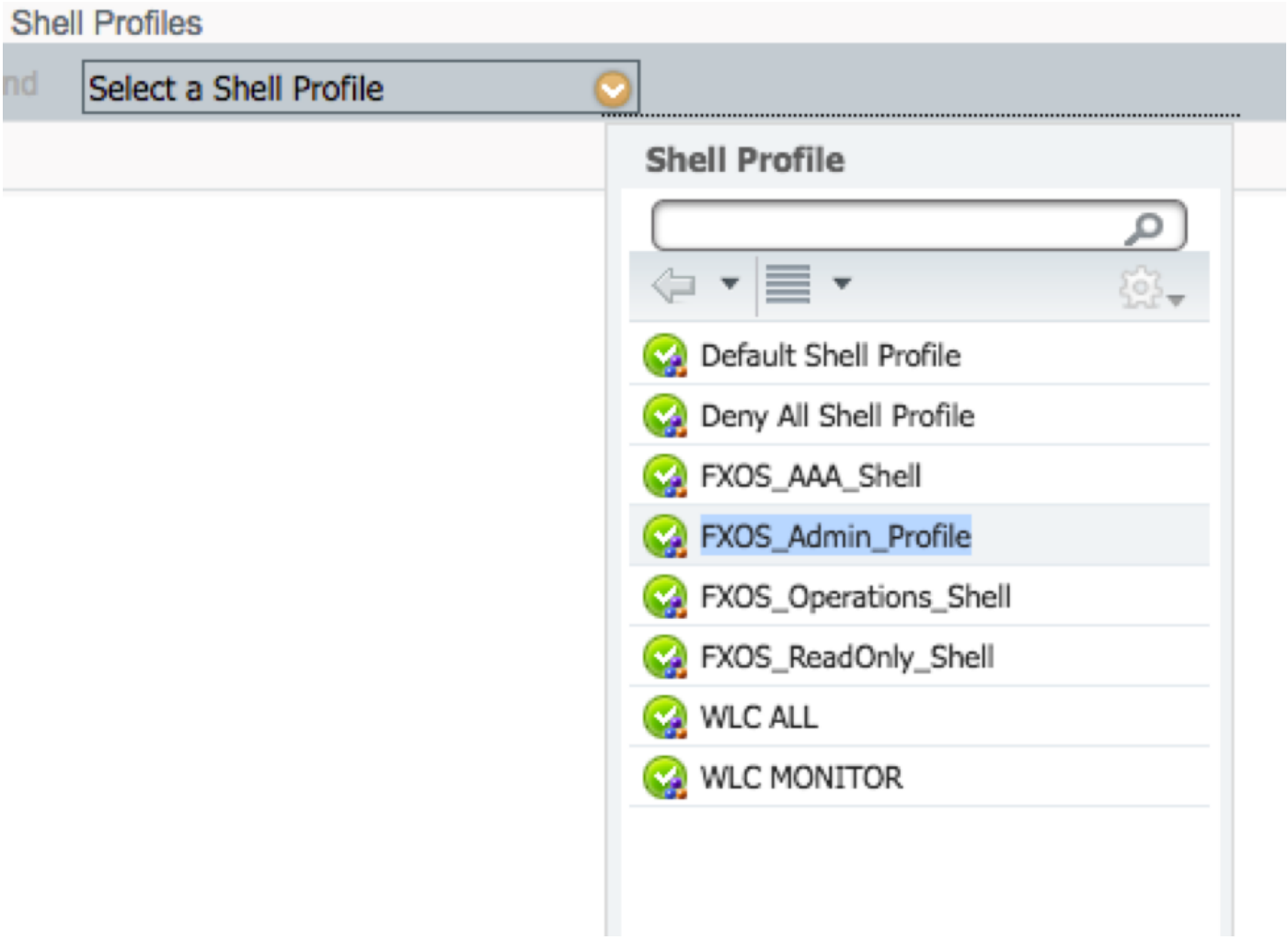
如果：使用者身份組為FXOS管理員



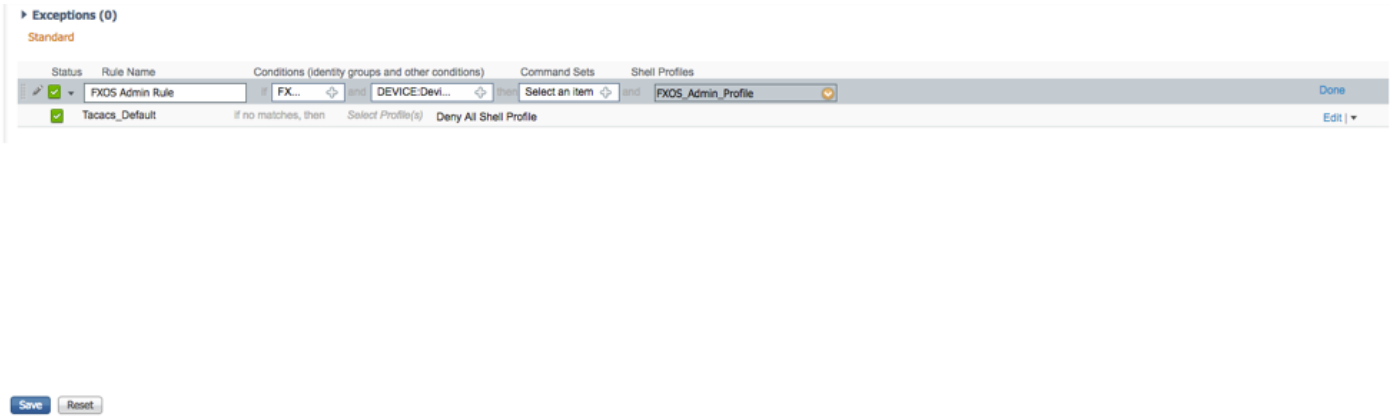
和裝置：裝置型別等於所有裝置型別#FXOS



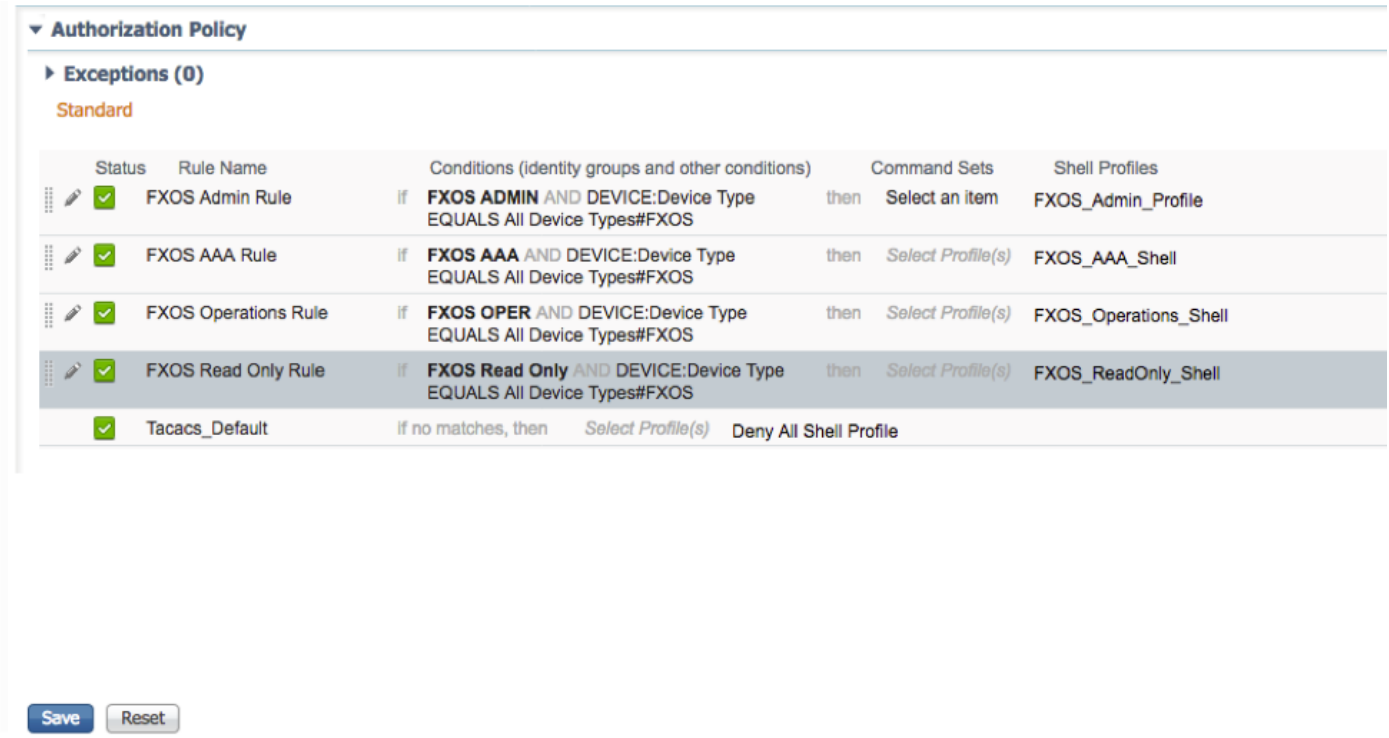
外殼配置檔案：FXOS_Admin_Profile



步驟5.按一下「**Done**」。



步驟6.對其餘使用者角色重複步驟3和步驟4，並在完成後按一下**SAVE**。



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訪問FXOS機箱，然後使用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

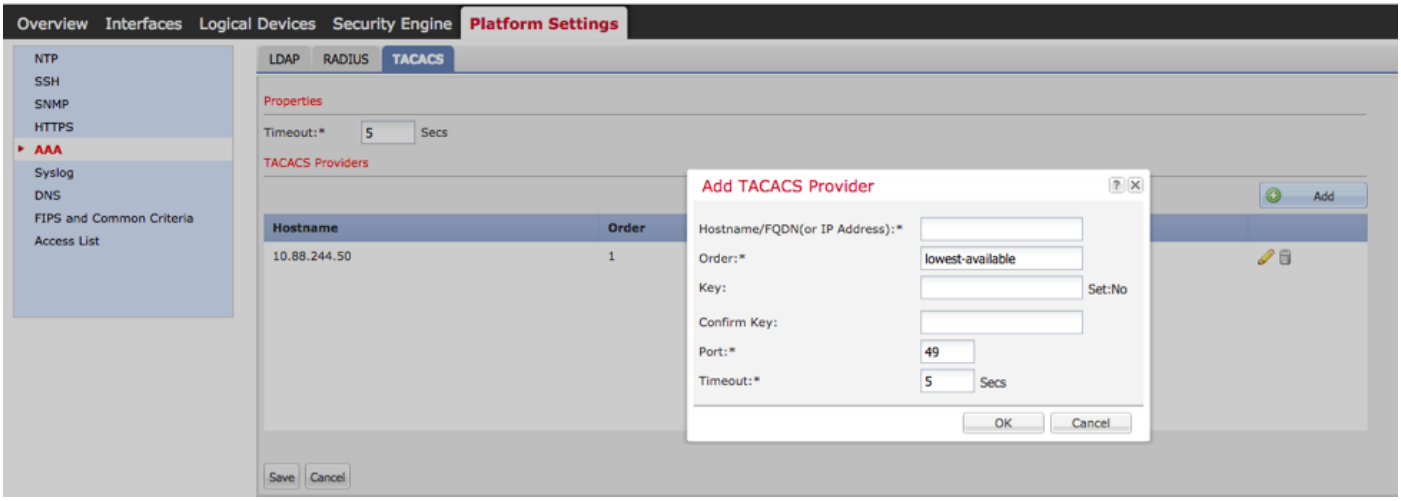
fpr4120-TAC-A#connect **fxos**

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

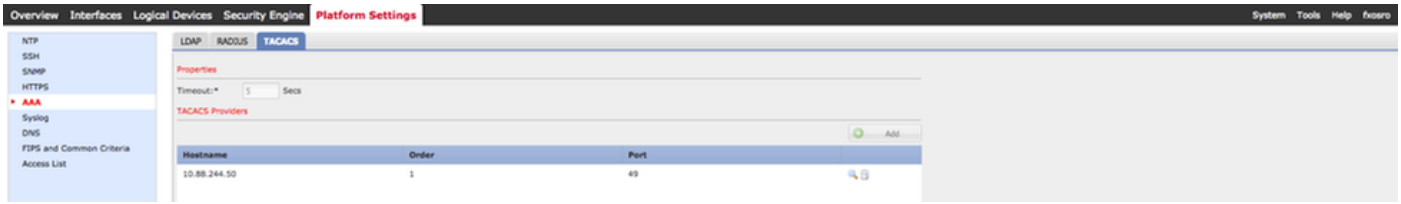
%角色許可權被拒絕

2.瀏覽到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。



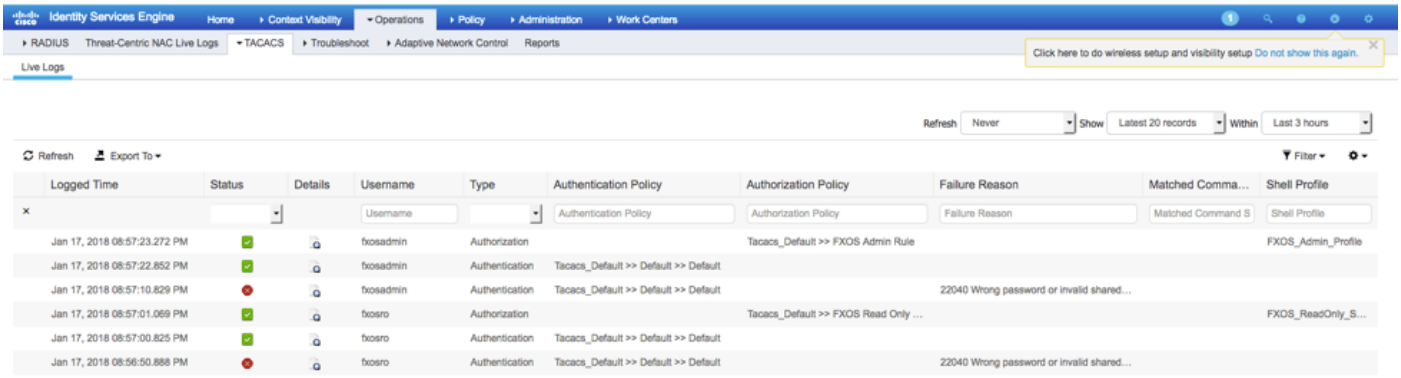
只讀使用者角色。



附註：請注意， **ADD**按鈕呈灰色顯示。

ISE 2.0

1.**Operations > TACACS Livelog**



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17日15:46:40.305247 aaa:用於身份驗證的aaa_req_process。會話編號0

2018年1月17日15:46:40.305262 aaa:aaa_req_process:來自裝置的常規AAA請求：login appn_subtype:預設

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:配置的方法總數為1，要嘗試的當前索引為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:使用傳遞到此函式的sg_protocol

2018年1月17日15:46:40.305324 aaa:正在向TACACS服務傳送請求

2018年1月17日15:46:40.305384 aaa:配置的方法組成功

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響應

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

2018年1月17日15:46:40.557042 aaa:會話：0x8dfd68c已從會話表0中刪除

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

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

2018年1月17日15:46:40.557075 aaa:用於身份驗證的aaa_send_client_response。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:用於授權的aaa_req_process。會話編號0

2018年1月17日15:46:40.557378 aaa:使用來自應用程式的上下文呼叫aaa_req_process:login appn_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 group =（空）

2018年1月17日15:46:40.557401 aaa:使用傳遞到此函式的sg_protocol

2018年1月17日15:46:40.557408 aaa:基於上下文或定向AAA請求(異常：不是中繼請求)。 將不獲取aaa請求的副本

2018年1月17日15:46:40.557415 aaa:正在向TACACS服務傳送請求

2018年1月17日15:46:40.801732 aaa:用於授權的aaa_send_client_response。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:舊操作碼：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 the role:admin

2018年1月17日15:46:40.848963 aaa:aaa_req_process用於記帳。會話編號0

2018年1月17日15:46:40.848972 aaa:MTS請求引用為空。LOCAL請求

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

2018年1月17日15:46:40.848992 aaa:aaa_req_process:來自裝置的常規AAA請求：default appln_subtype:預設

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:沒有針對預設預設配置的方法

2018年1月17日15:46:40.849032 aaa:沒有可用於此請求的配置

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:update:::added user:fxosadmin至role:admin

身份驗證嘗試失敗後，您將看到以下輸出。

2018年1月17日15:46:17.836271 aaa:用於身份驗證的aaa_req_process。會話編號0

2018年1月17日15:46:17.836616 aaa:aaa_req_process:來自裝置的常規AAA請求：login appn_subtype:預設

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:配置的方法總數為1，要嘗試的當前索引為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:使用傳遞到此函式的sg_protocol

2018年1月17日15:46:17.839167 aaa:正在向TACACS服務傳送請求

2018年1月17日15:46:17.840225 aaa:配置的方法組成功

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

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

2018年1月17日15:46:18.044395 aaa:用於身份驗證的aaa_send_client_response。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:請求消息的mts_drop

2018年1月17日15:46:18.045699 aaa:應釋放aaa_req。

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登入錯誤消息

2018年1月17日15:46:18.045738 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Ethanalyzer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