Firepower eXtensible Operating System(FXOS)2.2:TACACS+を使用したISEによるリモート管理のためのシャーシ認証/許可

内容

概要

このドキュメントでは、Identity Services Engine(ISE)を介してFirepower eXtensible Operating System(FXOS)シャーシのTACACS+認証および認可を設定する方法について説明します。

FXOSシャーシには、次のユーザロールが含まれます。

- 管理者：システム全体への読み取り/書き込みアクセスを完了します。デフォルトの管理者アカウントにはデフォルトでこのロールが割り当てられ、変更できません。
- 読み取り専用：システムの状態を変更する権限のない、システム設定への読み取り専用アクセス。
- 操作：NTP設定、スマートライセンス用のSmart Call Home設定、システムログ（syslogサーバと障害を含む）への読み取りと書き込みのアクセス。システムの残りの部分への読み取りアクセス。
- AAA：ユーザ、ロール、およびAAA設定への読み取りおよび書き込みアクセス。システムの残りの部分への読み取りアクセス。

CLIでは、次のように表示できます。

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

ロール：

ロール名の特権

— —

aaa

admin admin

運用業務

読み取り専用

著者：Cisco TACエンジニア、Tony Remirez、Jose Soto

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Firepower eXtensible Operating System(FXOS)に関する知識
- ISE設定に関する知識
- TACACS+デバイス管理ライセンスがISE内に必要

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Firepower 4120セキュリティアプライアンスバージョン2.2
- 仮想Cisco Identity Services Engine(ISE)2.2.0.470

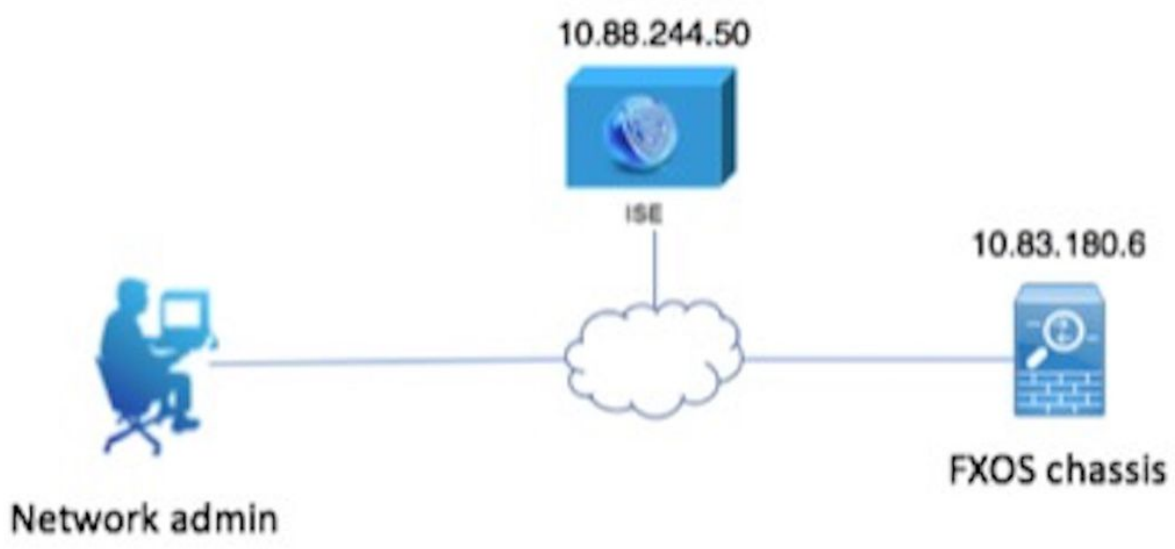
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

設定の目的は次のとおりです。

- ISEを使用して、FXOSのWebベースGUIおよびSSHにログインするユーザを認証します
- ISEを使用して、FXOSのWebベースGUIおよびSSHにログインするユーザを、それぞれのユーザロールに従って許可します。
- ISEを使用したFXOSでの認証と認可の適切な動作の確認

ネットワーク図



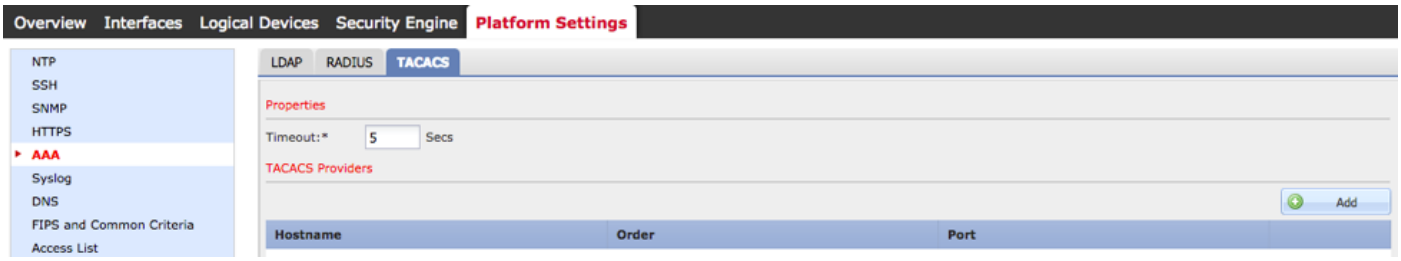
設定

FXOSシャーシの設定

TACACS+プロバイダーの作成

ステップ1:[Platform Settings] > [AAA]に移動します。

ステップ2:[TACACS]タブをクリックします。

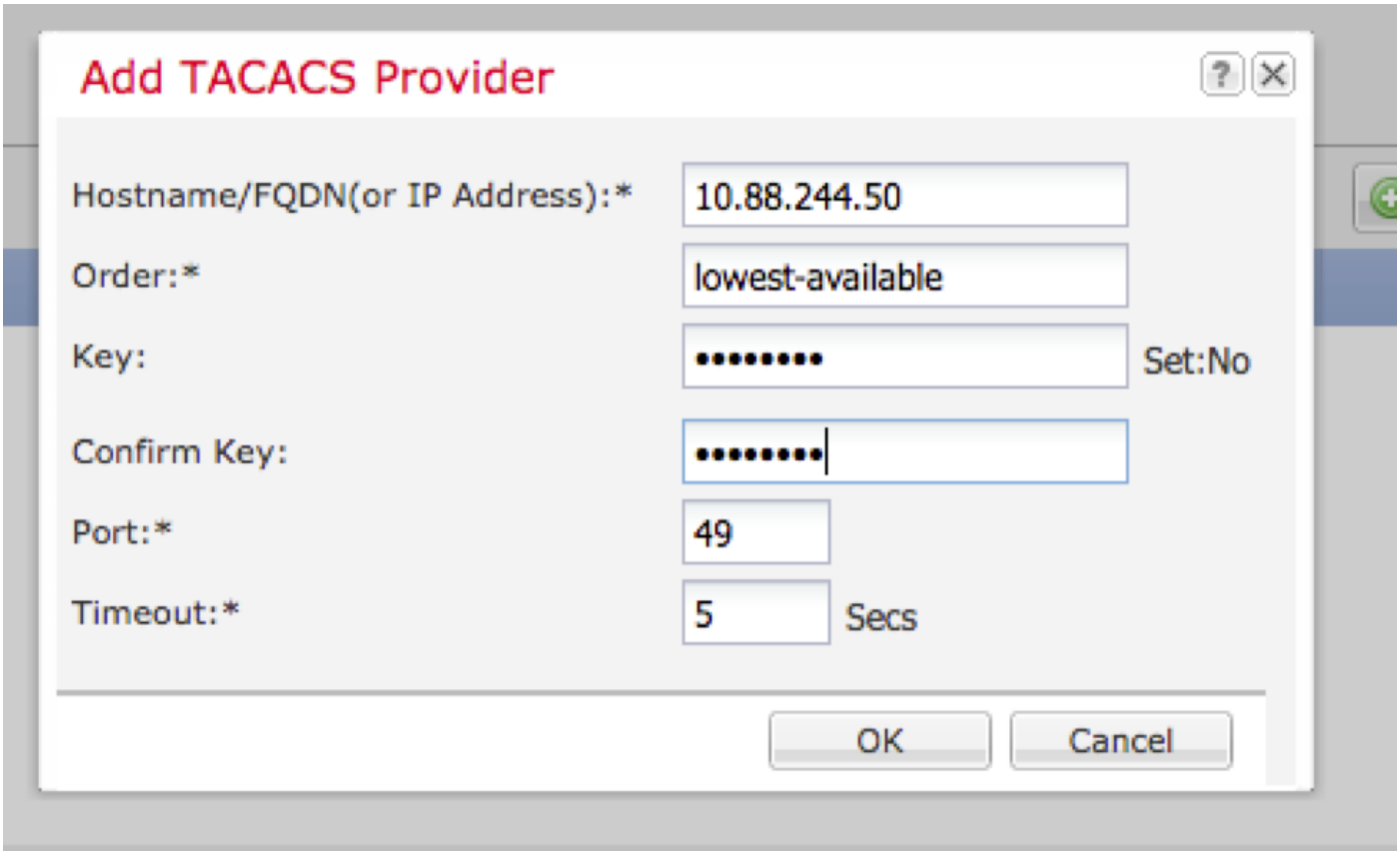


ステップ3：追加する各TACACS+プロバイダー（最大16プロバイダー）について。

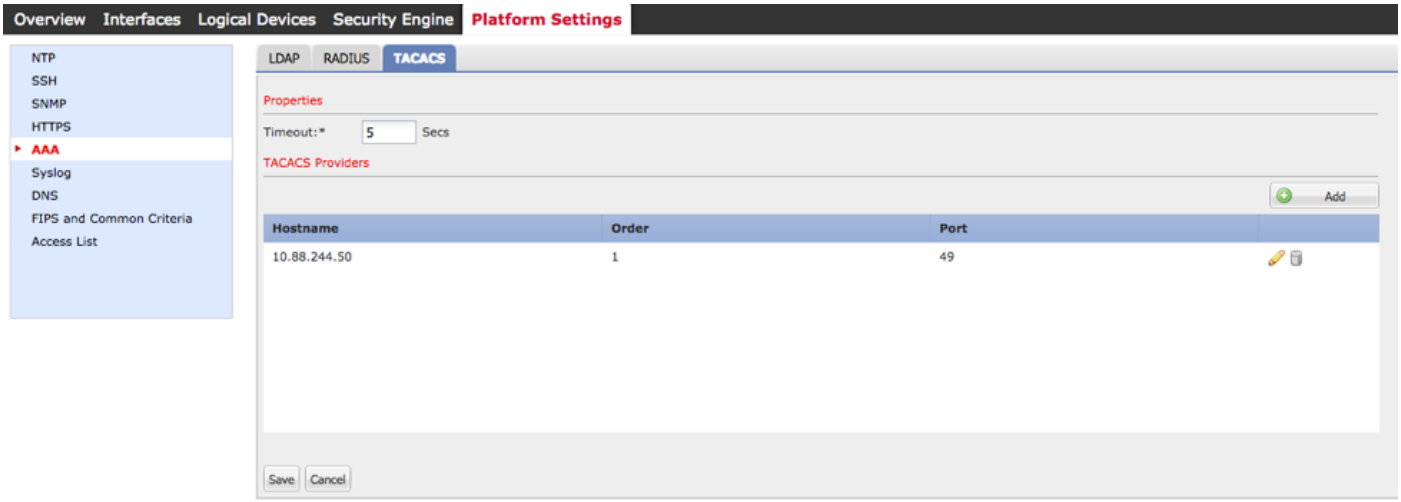
3.1. [TACACS Providers]領域で、[Add]をクリックします。

3.2. [Add TACACS Provider]ダイアログボックスが開いたら、必要な値を入力します。

3.3. 「OK」をクリックし、「TACACSプロバイダーの追加」ダイアログ・ボックスを閉じます。

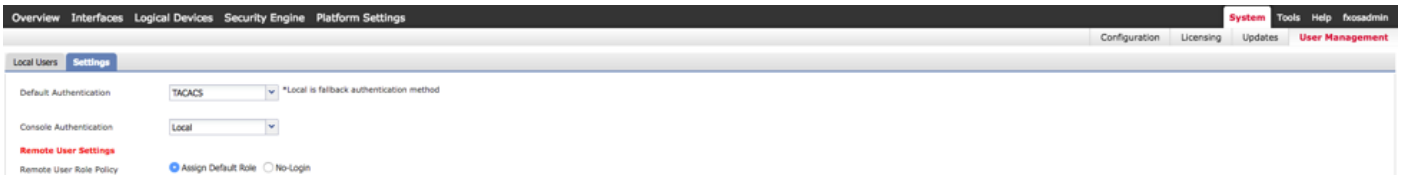


ステップ4:[Save]をクリックします。



ステップ5:[System] > [User Management] > [Settings]に移動します。

ステップ6:[Default Authentication]で[TACACS]を選択します。



CLIを使用したTACACS+プロバイダーの作成

ステップ1:TACACS認証を有効にするには、次のコマンドを実行します。

fpr4120-TAC-A#スコープセキュリティ

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

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

ステップ2:**show detailコマンド**を使用して設定を確認します。

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

デフォルト認証：

管理レルム：**TACACS**

動作領域：**TACACS**

Webセッションの更新間隔（秒）:600

Web、ssh、telnetセッションのセッションタイムアウト（秒）:600

Web、ssh、telnetセッションの絶対セッションタイムアウト（秒）:3600

シリアルコンソールセッションのタイムアウト（秒）:600

シリアルコンソールの絶対セッションタイムアウト（秒）:3600

管理認証サーバグループ：

動作認証サーバグループ：

2次係数の使用：No

ステップ3:TACACSサーバパラメータを設定するには、次のコマンドを実行します。

fpr4120-TAC-A#スコープセキュリティ

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**

キーを入力します。******

キーを確認します。******

ステップ4:**show detailコマンド**を使用して設定を確認します。

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

TACACS+サーバ：

ホスト名、FQDN、またはIPアドレス：10.88.244.50

descr　　：

発注：1

[Port]：49

ポイント：****

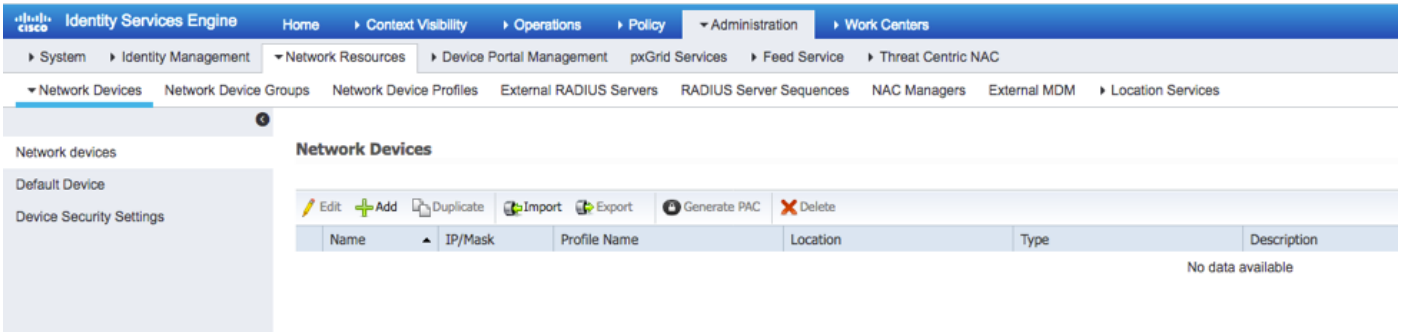
タイムアウト：5

ISEサーバの設定

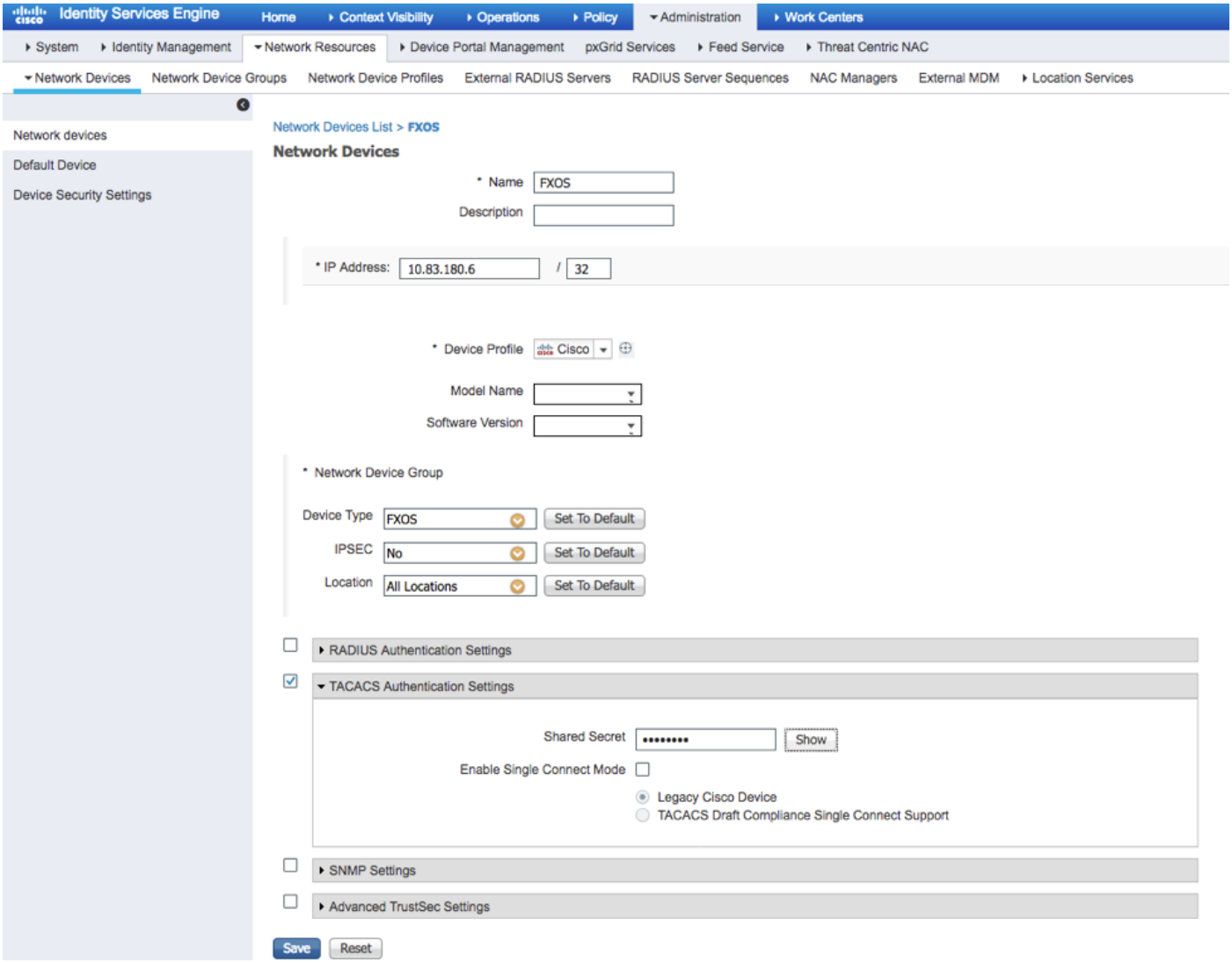
ネットワークリソースとしてのFXOSの追加

ステップ1:[Administration] > [Network Resources] > [Network Devices]の順に移動します。

ステップ2:[ADD]をクリックします。



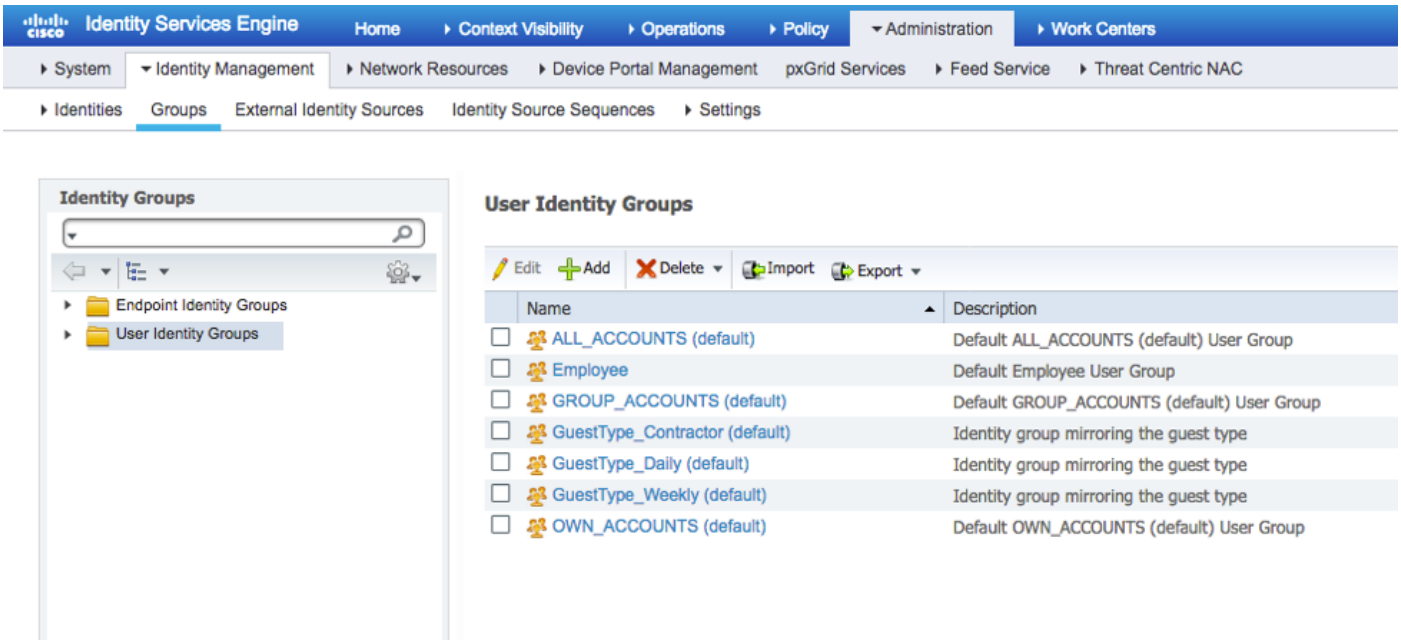
ステップ3：必要な値([Name]、[IP Address]、[Device Type]、[Enable TACACS+])を入力し、[Submit]をクリックします。



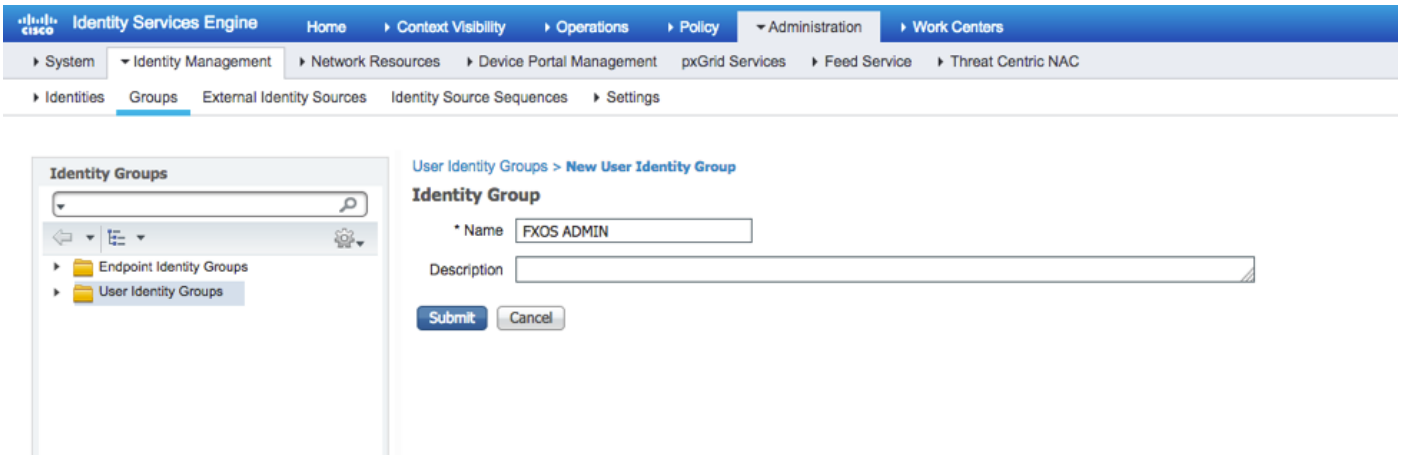
アイデンティティグループとユーザの作成

ステップ1:[Administration] > [Identity Management] > [Groups] > [User Identity Groups]に移動します。

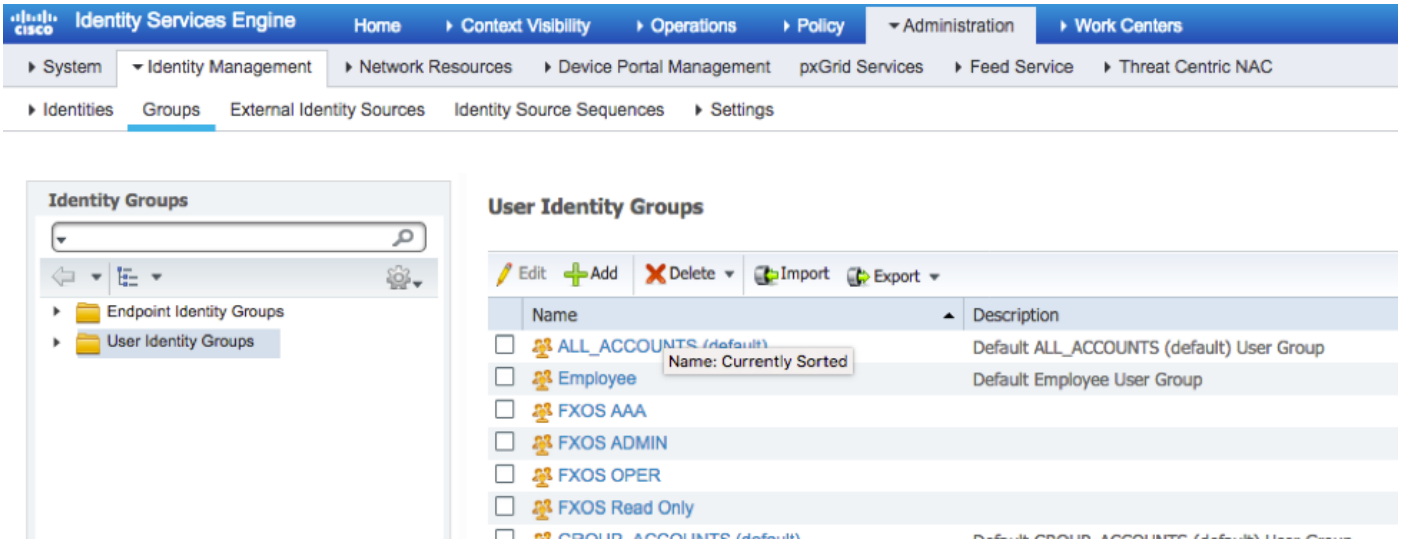
ステップ2:[ADD]をクリックします。



ステップ3:[Name]に値を入力し、[Submit]をクリックします。

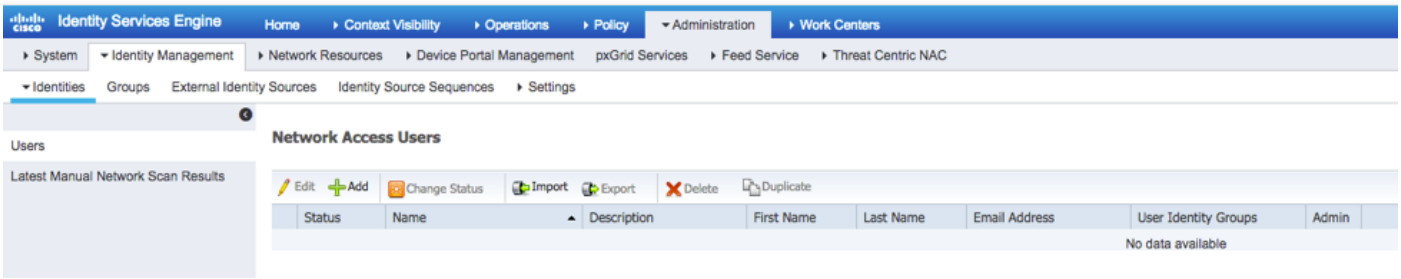


ステップ4：必要なすべてのユーザロールについて、ステップ3を繰り返します。

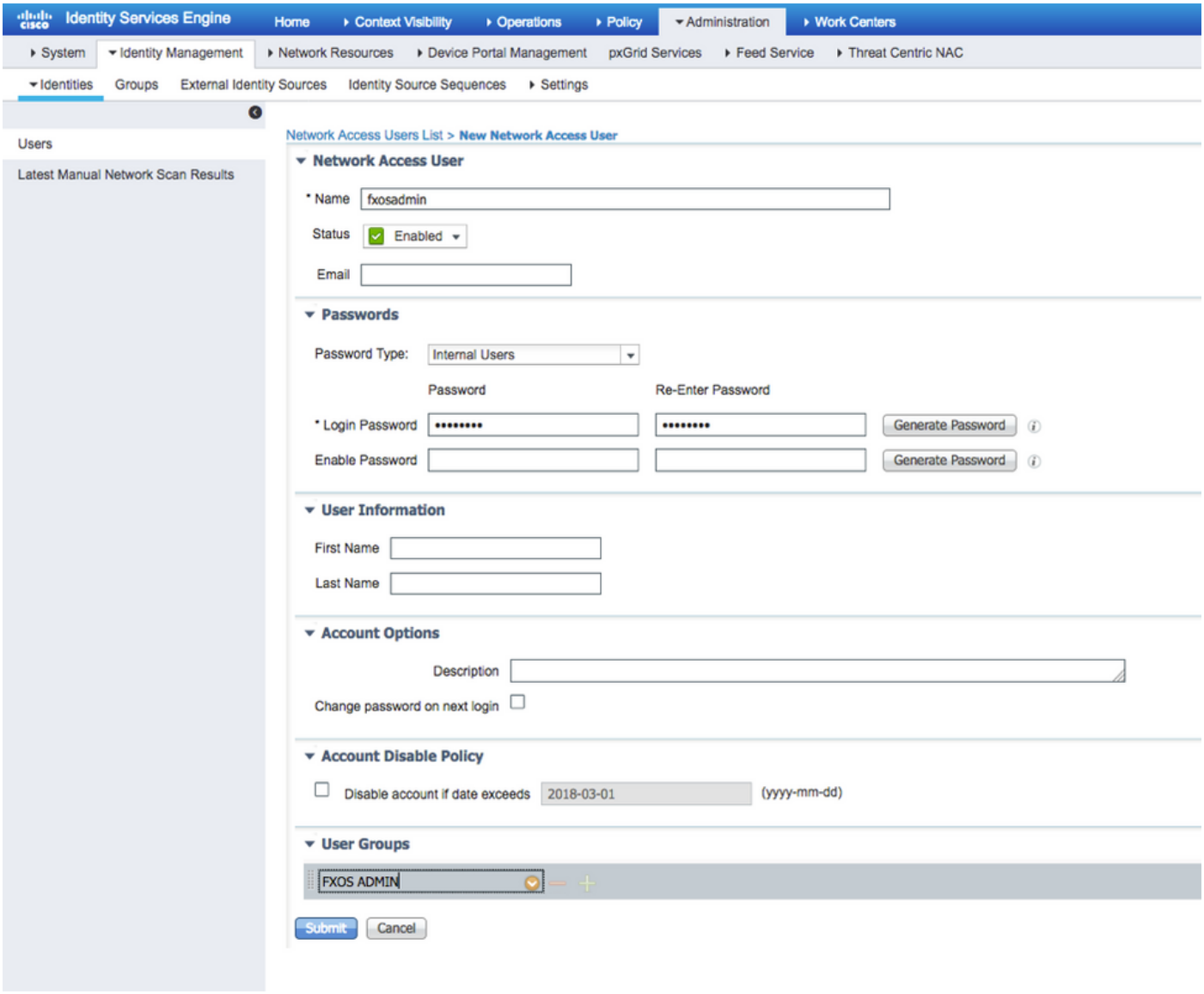


ステップ5:[Administration] > [Identity Management] > [Identity] > [Users]に移動します。

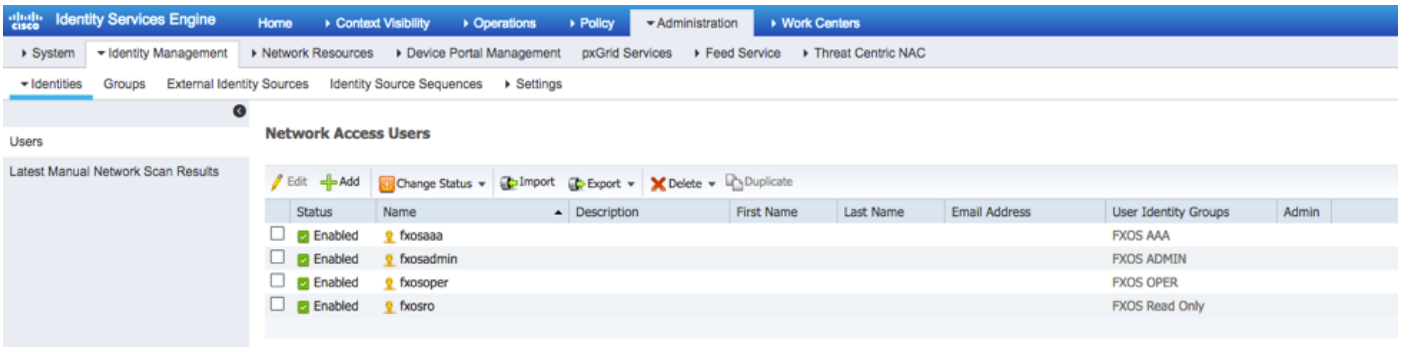
ステップ6:[ADD]をクリックします。



ステップ7：必要な値（名前、ユーザグループ、パスワード）を入力します。

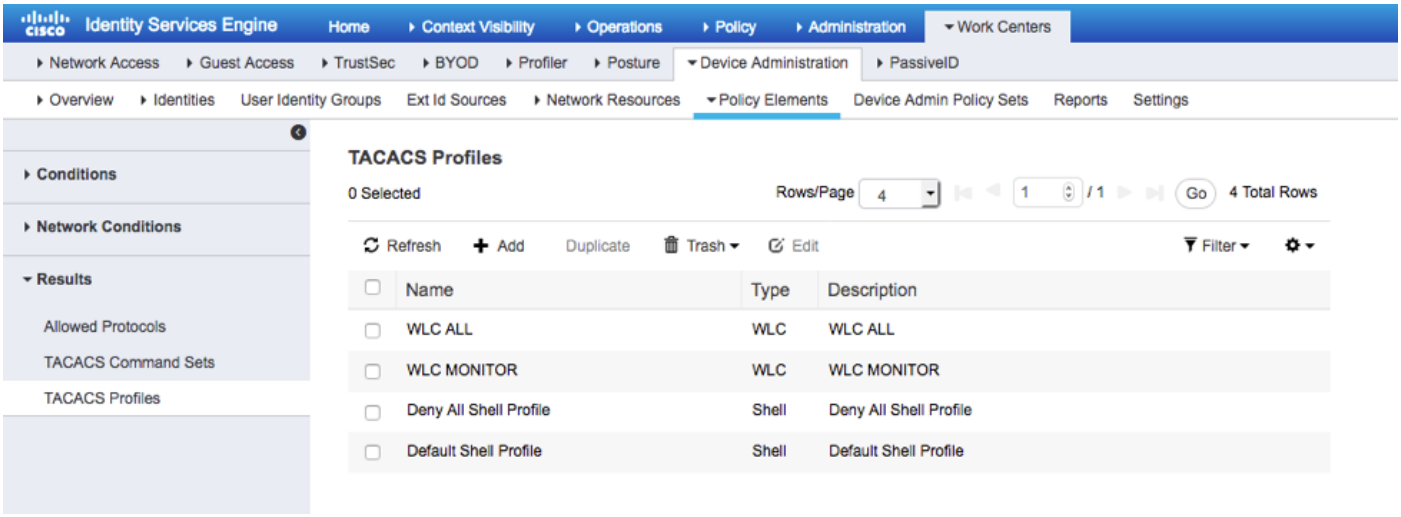


ステップ8：必要なすべてのユーザに対してステップ6を繰り返します。



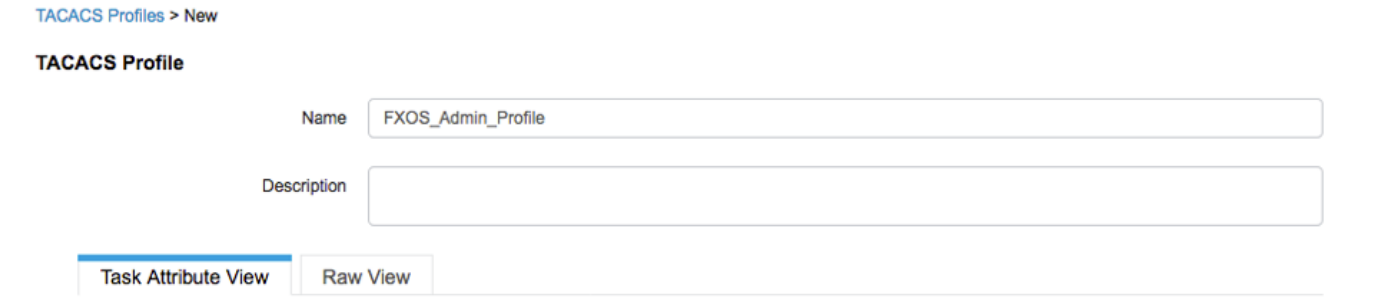
各ユーザロールのシェルプロファイルの作成

ステップ1:[Work Centers] > **[Device Administration] > [Policy Elements] > [Results] > [TACACS Profiles]に移動し、[+ ADD]をクリックします。**



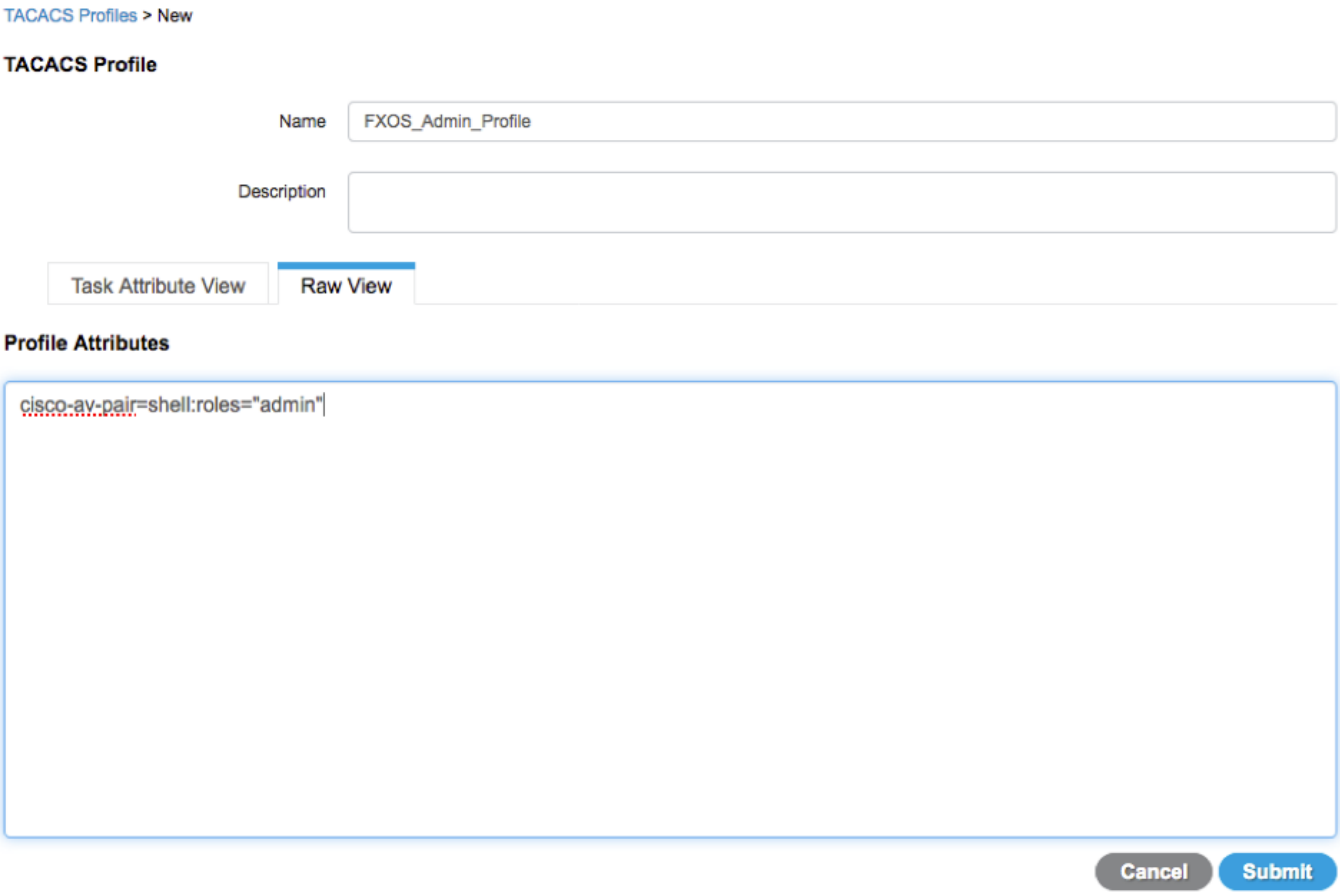
ステップ2:TACACSプロファイルに必要な値を入力します

2.1. [Name]を入力します。

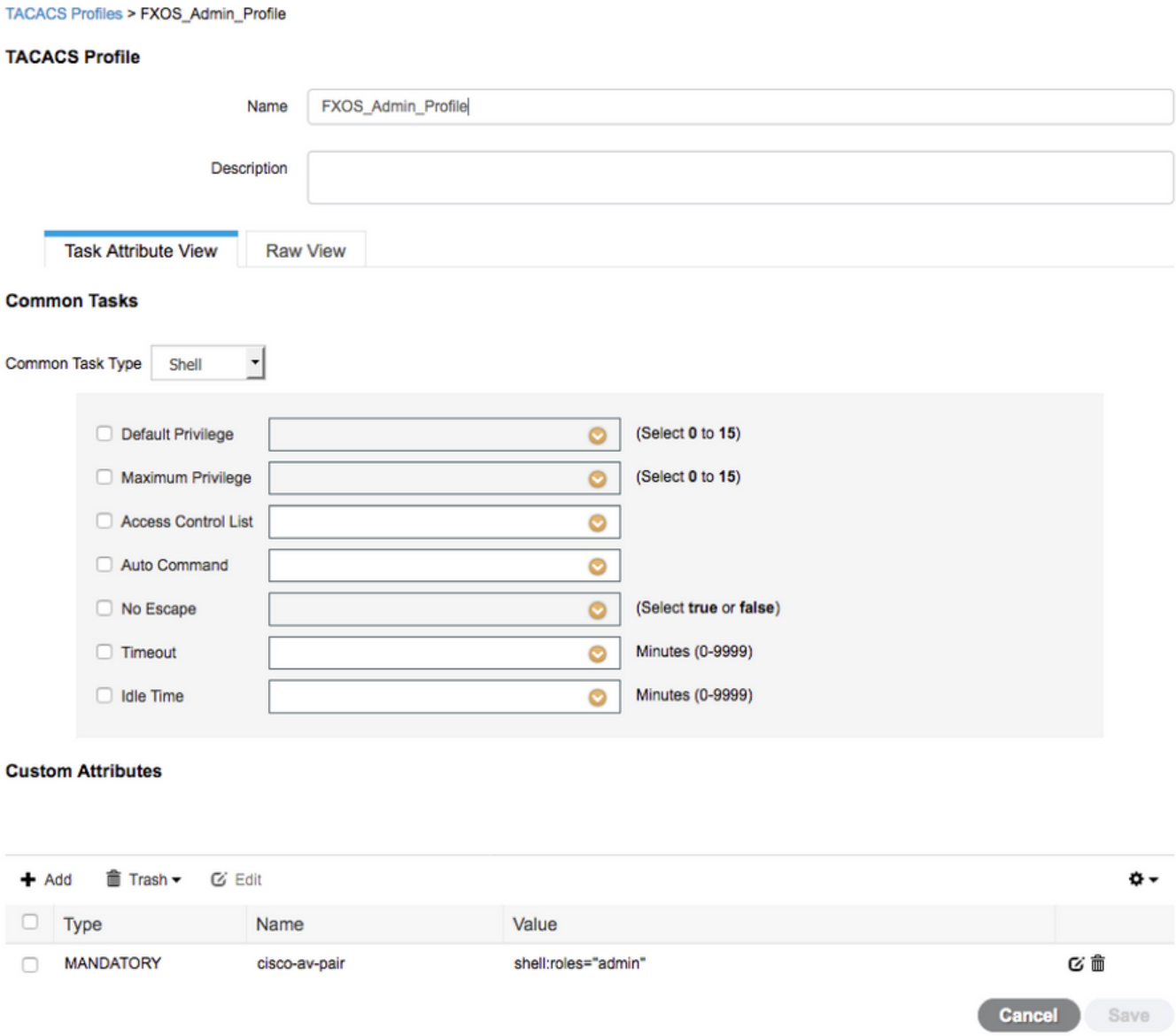


2.2. [RAW View]**タブで**、次のCISCO-AV-PAIRを設定します。

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



2.3. [送信]をクリックします。

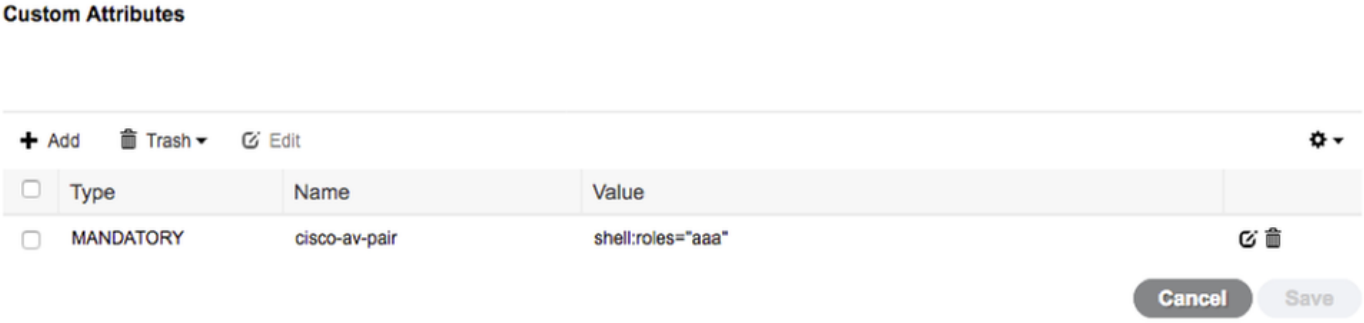


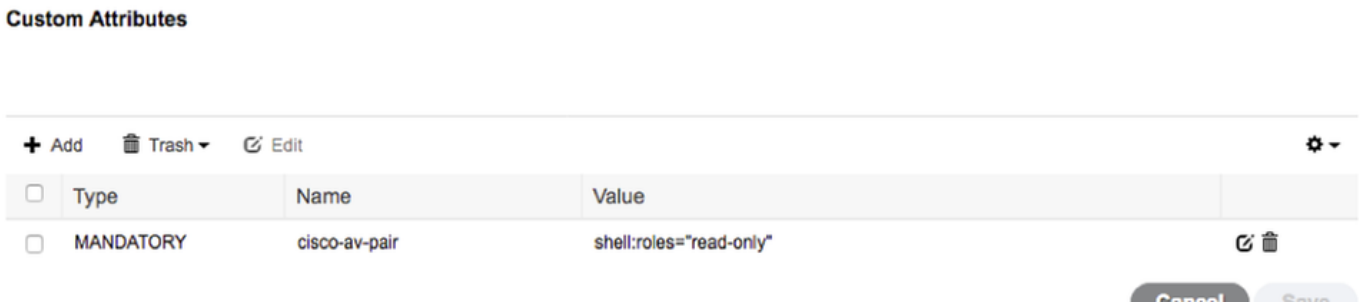
ステップ3：次のCisco-AV-Pairsを使用して、残りのユーザロールについてステップ2を繰り返します。

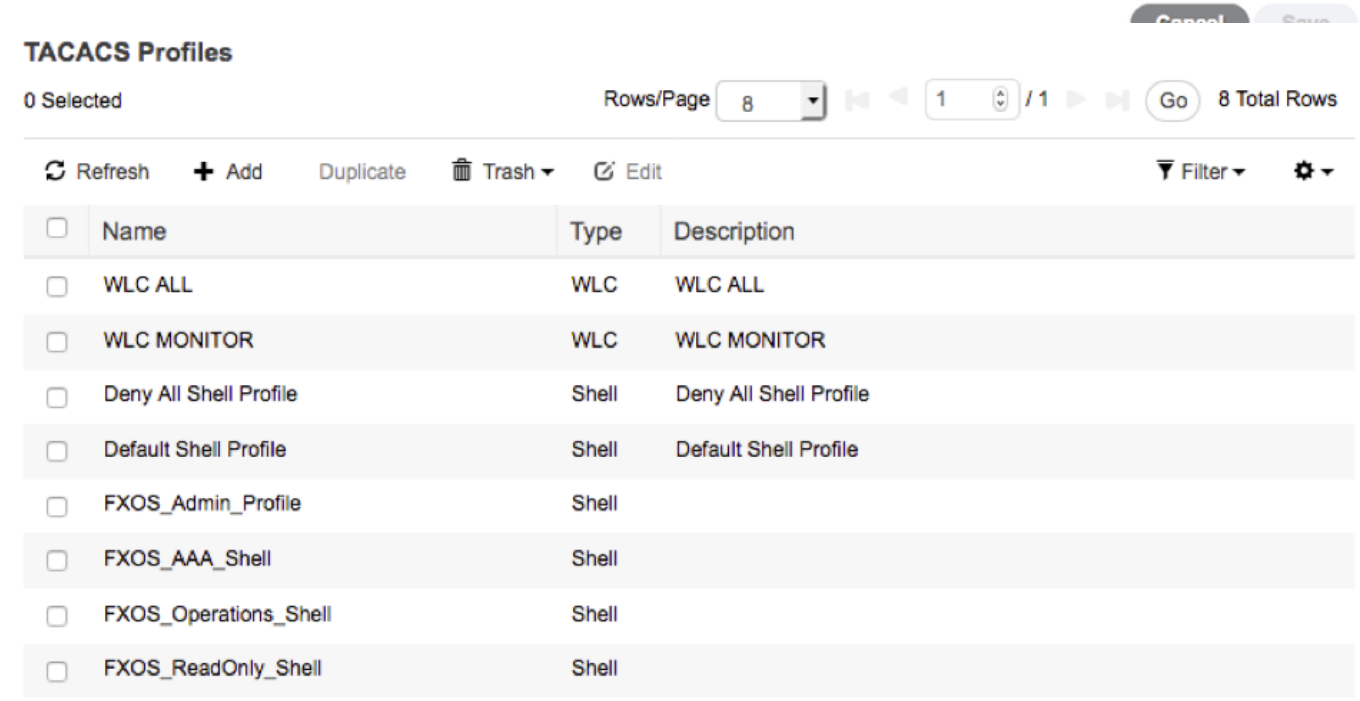
cisco-av-pair=shell:roles="aaa"

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

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

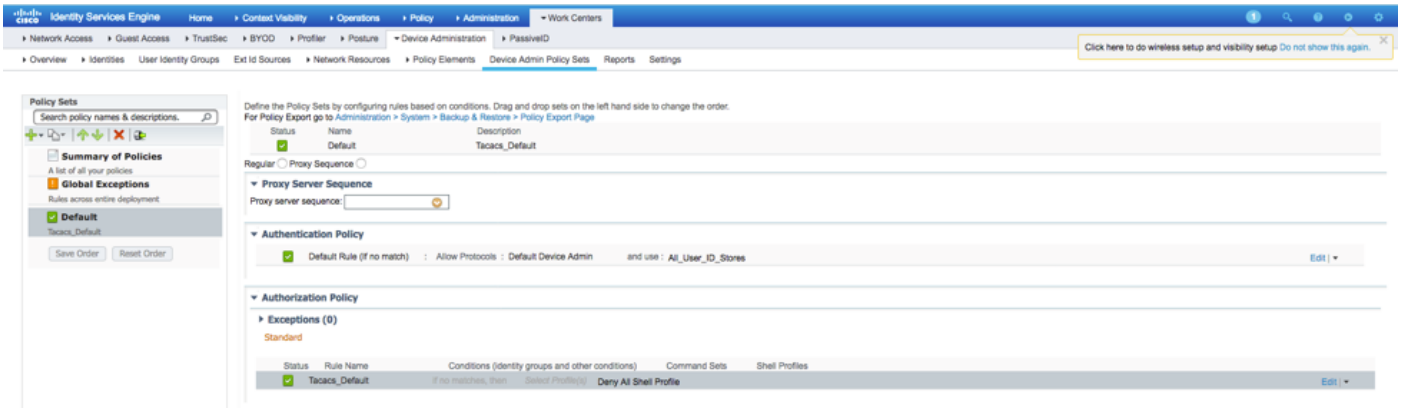




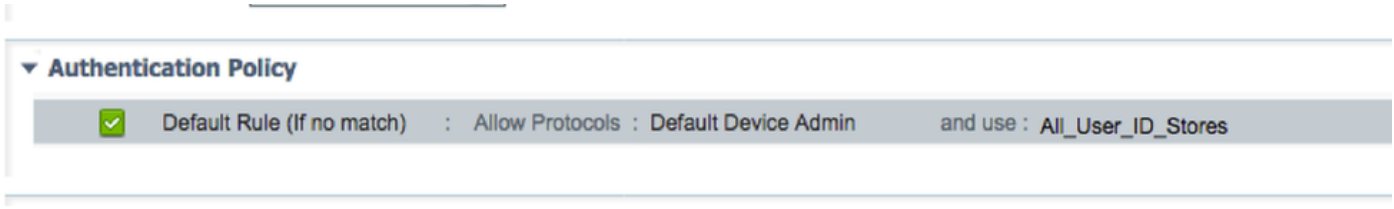


TACACS認可ポリシーの作成

ステップ1:[Work Centers] > **[Device Administration] > [Device Admin Policy Sets]に移動します。**



ステップ2：認証ポリシーが内部ユーザデータベースまたは必要なIDストアを指していることを確認します。



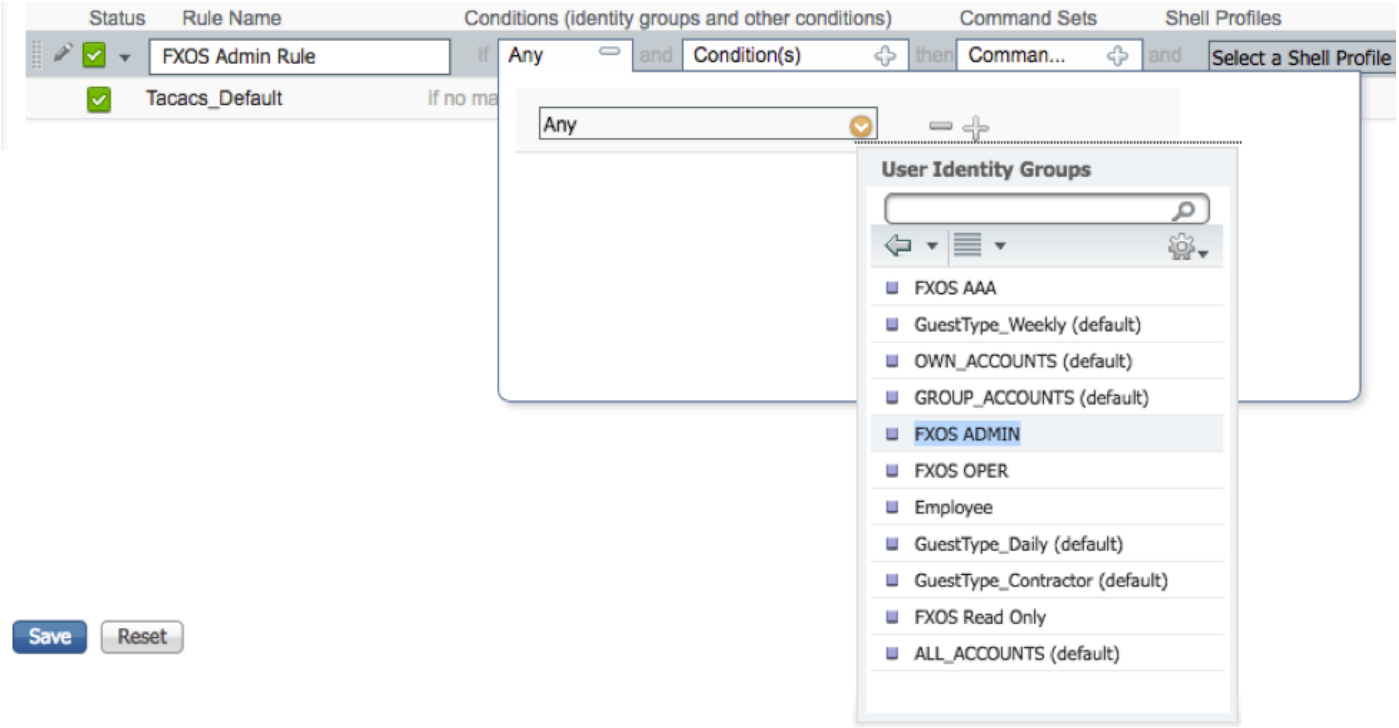
ステップ3：デフォルトの認可ポリシーの最後にある矢印をクリックし、上の[Insert rule]をクリックします。

ステップ4：必要なパラメータを使用して、ルールの値を入力します。

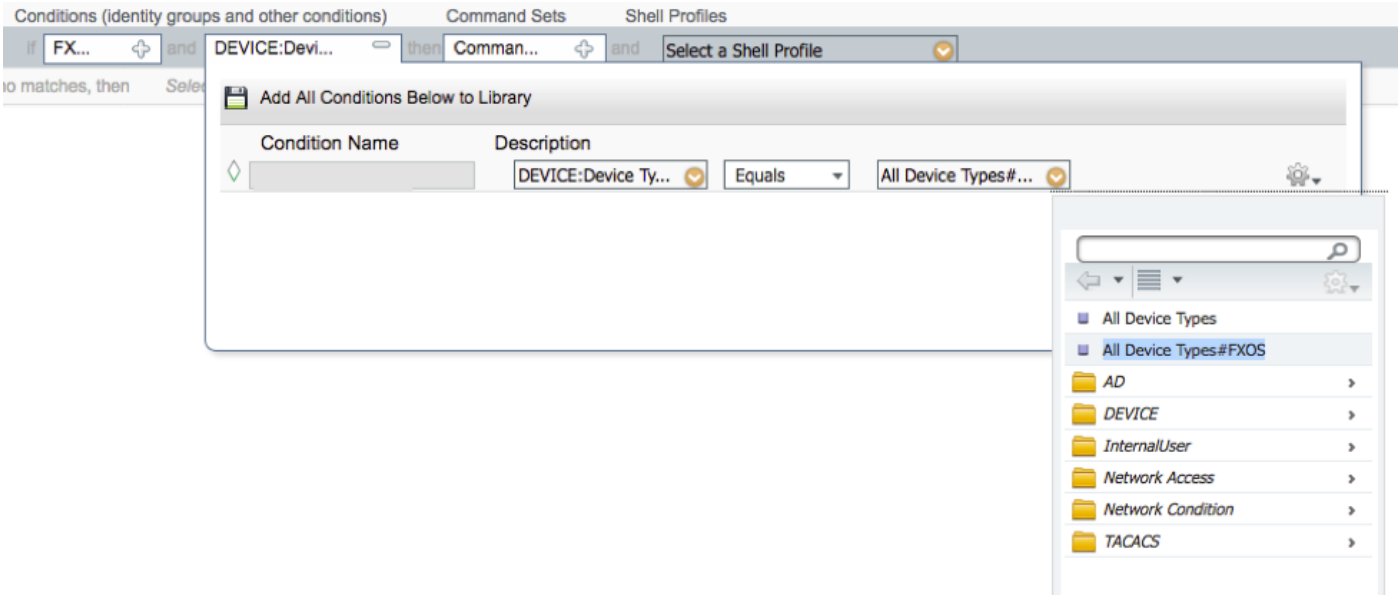
4.1.ルール名：FXOS管理規則。

4.2条件

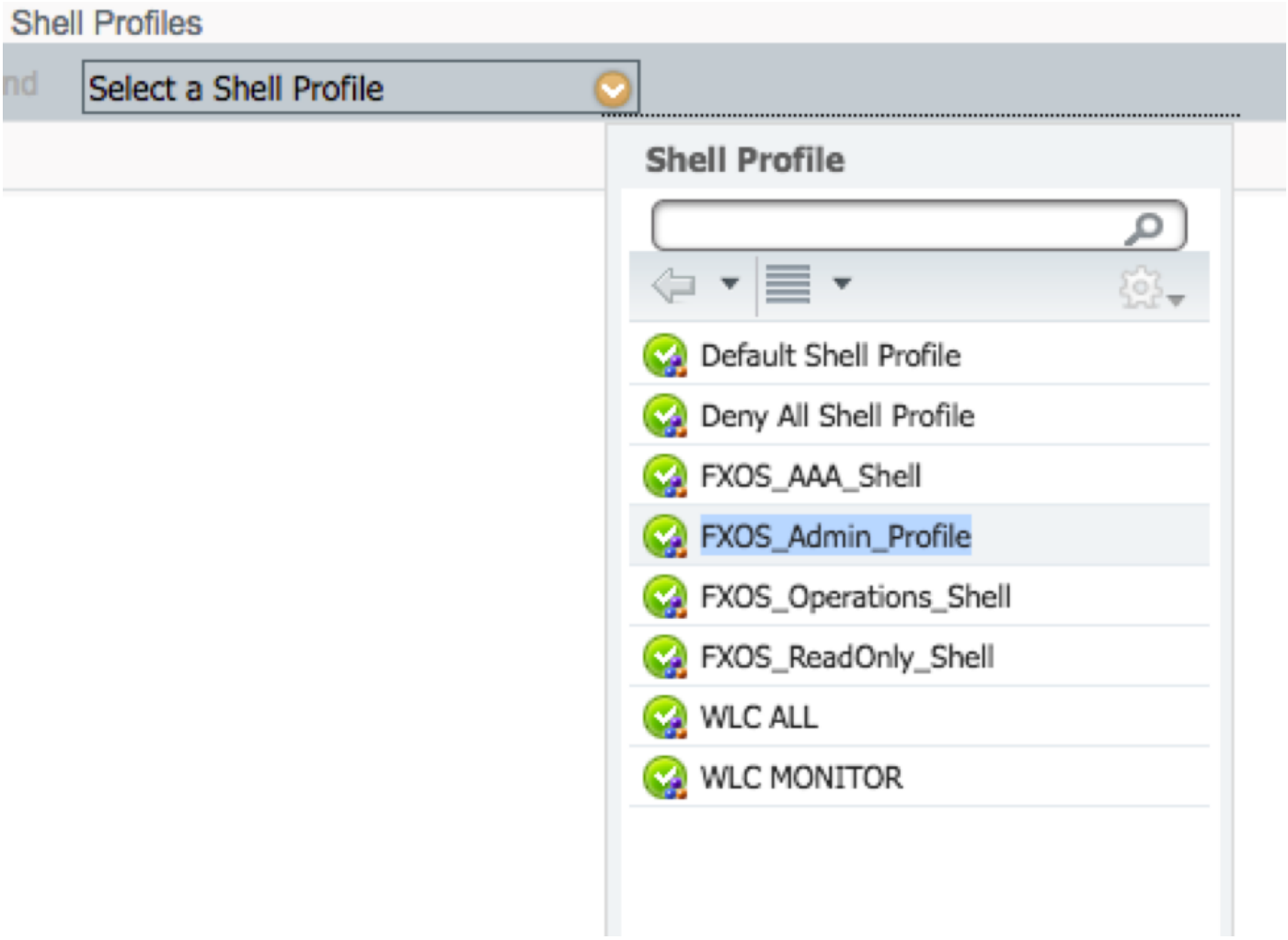
条件ユーザIDグループはFXOS ADMINです



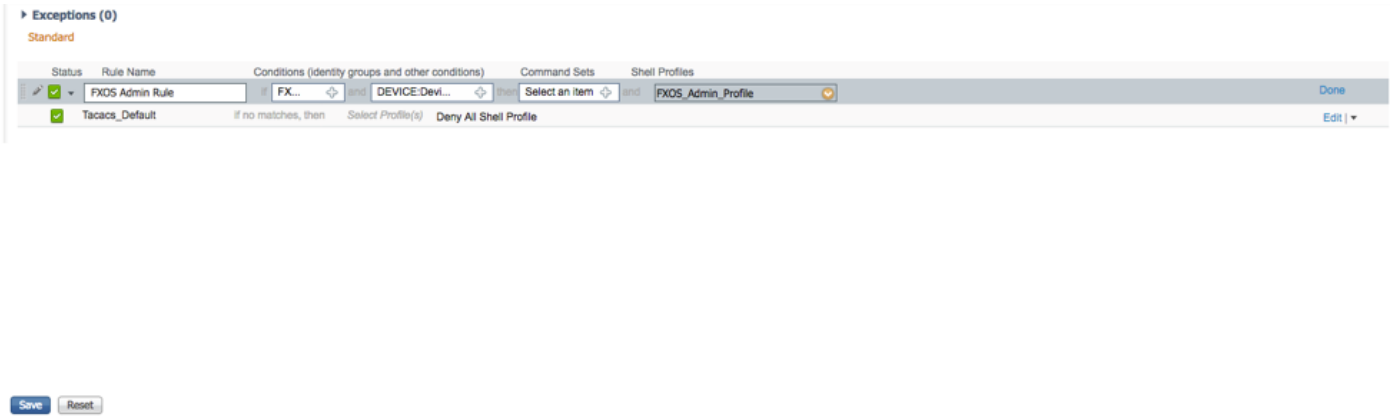
およびデバイス：[Device Type]は[All Device Types]#FXOSです。



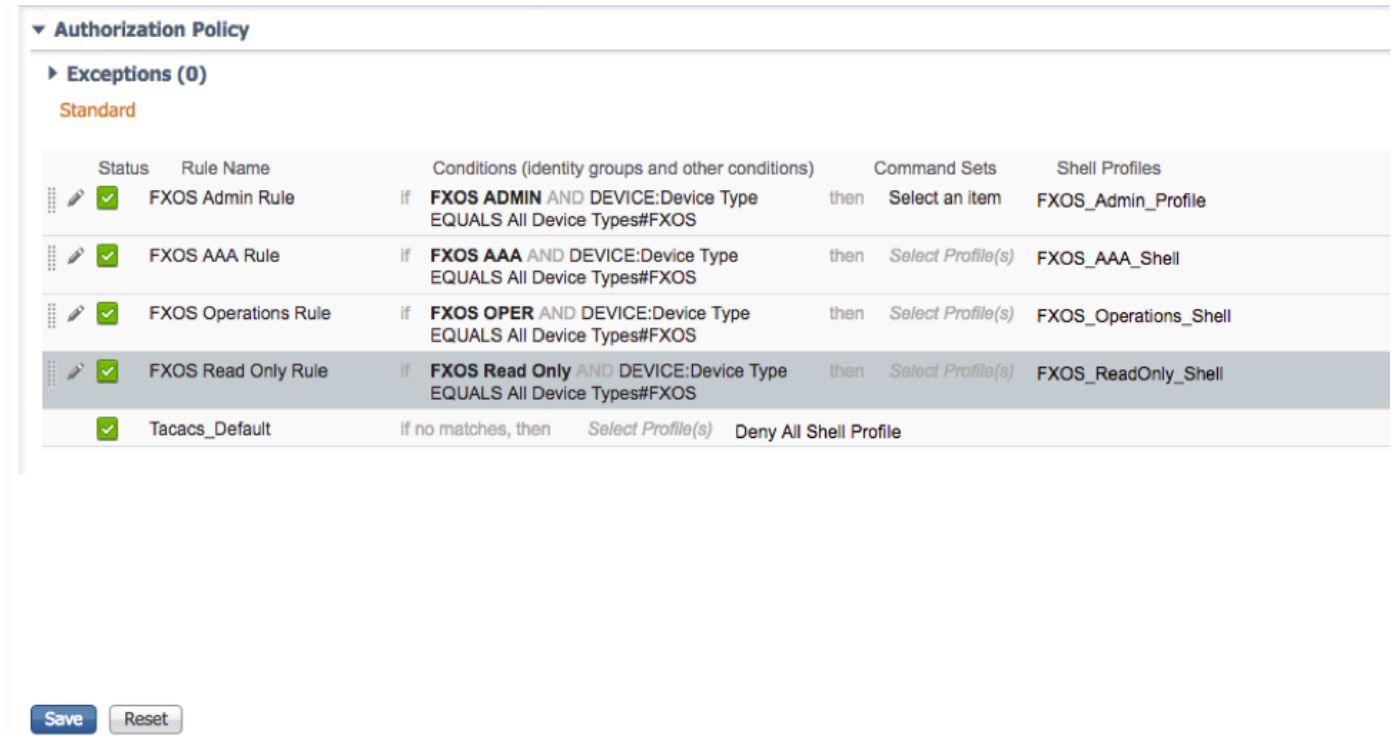
シェルプロファイル：FXOS_Admin_Profile



ステップ5:[完了]をクリックします。



ステップ6：残りのユーザロールについてステップ3と4を繰り返し、完了したら[SAVE]をクリックします。



確認

各ユーザをテストし、割り当てられたユーザロールを確認できます。

FXOSシャーシ検証

1. FXOSシャーシにTelnetまたはSSHで接続し、ISEで作成したユーザのいずれかを使用してログインします。

ユーザ名:fxosadmin

パスワード：

fpr4120-TAC-A#スコープセキュリティ

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

リモートユーザーfxosa:

説明:

ユーザ ロール:

[Name]：[AAA]

[Name]：読み取り専用

リモートユーザーfxosadmin:

説明:

ユーザ ロール:

[Name]：admin

[Name]：読み取り専用

リモートユーザーフソッパー:

説明:

ユーザ ロール:

[Name]：運用

[Name]：読み取り専用

リモートユーザーfxosro:

説明:

ユーザ ロール:

[Name]：読み取り専用

FXOSシャーシのcliに入力したユーザ名に応じて、割り当てられたユーザロールに対して許可されたコマンドだけが表示されます。

管理者ユーザロール。

fpr4120-TAC-A /security # ?

確認応答

clear-user-sessions Clear User Sessions

管理対象オブジェクトの作成

管理オブジェクトの削除

disableサービスを無効にします

サービスの有効化

入力マネージオブジェクトを入力

scope現在のモードを変更する

プロパティ値の設定

show system information

アクティブなcimcセッションの終了

fpr4120-TAC-A#connect fxos

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

fpr4120-TAC-A(fxos)#

読み取り専用ユーザロール。

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

scope現在のモードを変更する

プロパティ値の設定

show system information

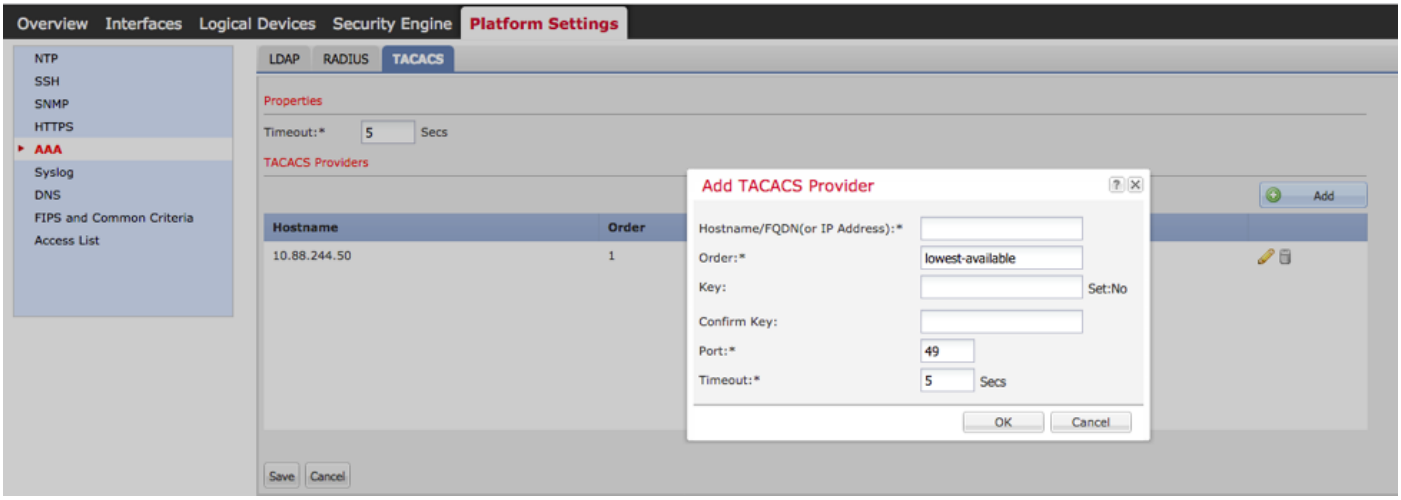
fpr4120-TAC-A#connect fxos

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

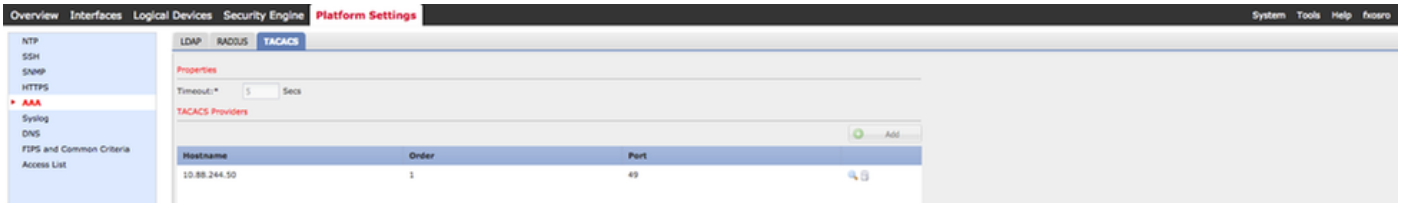
%権限が拒否されました

2. FXOSシャーシのIPアドレスを参照し、ISEで作成したユーザのいずれかを使用してログインします。

管理者ユーザロール。



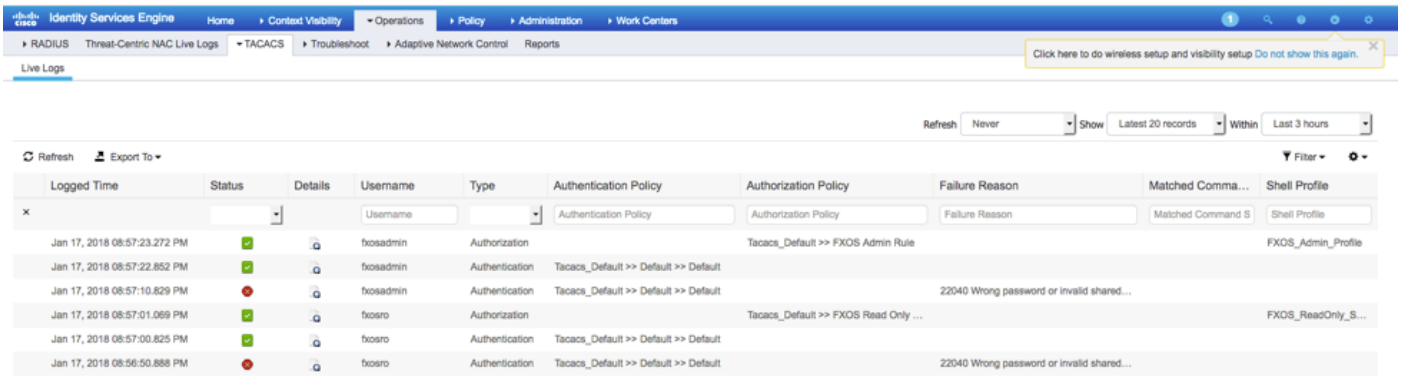
読み取り専用ユーザロール。



注：[ADD]ボタンがグレー表示されていることに注意してください。

ISE 2.0

1. [Operations] > [**TACACS Livelog**]



トラブルシュート

AAA認証と認可をデバッグするには、FXOS CLIで次のコマンドを実行します。

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**

認証に成功すると、次の出力が表示されます。

2018 Jan 17 15:46:40.305247 aaa:aaa_req_processを使用します。session no 0

2018 Jan 17 15:46:40.305262 aaa:aaa_req_process:applnからの一般的なAAA要求：login appln_subtype:default

2018 Jan 17 15:46:40.305271 aaa:try_next_aaa_method

2018 Jan 17 15:46:40.305285 aaa:設定されたメソッドの総数は1、試行される現在のインデックスは0

2018 Jan 17 15:46:40.305294 aaa:handle_req_using_method

2018 Jan 17 15:46:40.305301 aaa:AAA_METHOD_SERVER_GROUP

2018 Jan 17 15:46:40.305308 aaa:aaa_sg_method_handler group = tacacs

2018 Jan 17 15:46:40.305315 aaa:この関数に渡されるsg_protocolの使用

2018 Jan 17 15:46:40.305324 aaa:TACACSサービスへの要求の送信

2018 Jan 17 15:46:40.305384 aaa:構成されたメソッドグループが成功しました

2018 Jan 17 15:46:40.554631 aaa:aaa_process_fd_set

2018 Jan 17 15:46:40.555229 aaa:aaa_process_fd_set:aaa_qのmtscallback

2018 Jan 17 15:46:40.555817 aaa:mts_message_response_handler:mts応答

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

2018 Jan 17 15:46:40.557042 aaa:session:0x8dfd68cがセッションテーブル0から削除されました

2018 Jan 17 15:46:40.557059 aaa:is_aaa_resp_status_success status = 1

2018 Jan 17 15:46:40.557066 aaa:is_aaa_resp_status_successはTRUEです

2018年1月17 15:46:40.557075 aaa:aaa_send_client_responseを使用します。session->flags=21. aaa_resp->flags=0.

2018 Jan 17 15:46:40.557083 aaa:AAA_REQ_FLAG_NORMAL

2018 Jan 17 15:46:40.557106 aaa:mts_send_response成功

2018 Jan 17 15:46:40.557364 aaa:aaa_req_processを使用します。session no 0

2018 Jan 17 15:46:40.557378 aaa:aaa_req_process called with context from appln:login appln_subtype:default authen_type:2, authen_method:0

2018 Jan 17 15:46:40.557386 aaa:aaa_send_req_using_context

2018 Jan 17 15:46:40.557394 aaa:aaa_sg_method_handler group = (null)

2018 Jan 17 15:46:40.557401 aaa:この関数に渡されるsg_protocolの使用

2018 Jan 17 15:46:40.557408 aaa:コンテキストベースまたはダイレクトAAA要求(例外：リレー要求ではありません)。 AAA要求のコピーを取らない

2018 Jan 17 15:46:40.557415 aaa:TACACSサービスへの要求の送信

2018 Jan 17 15:46:40.801732 aaa:aaa_send_client_response（認可用）。session->flags=9. aaa_resp->flags=0

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

2018 Jan 17 15:46:40.801761 aaa:mts_send_response成功

2018 Jan 17 15:46:40.848932 aaa:古いOPCODE:accounting_interim_update

2018 Jan 17 15:46:40.848943 aaa:aaa_create_local_acct_req:user=、session_id=、log=added user:fxosadmin to role:admin

2018 Jan 17 15:46:40.848963 aaa:aaa_req_process（アカウンティング用）。session no 0

2018 Jan 17 15:46:40.848972 aaa:MTS要求参照がNULLです。ローカル要求

2018 Jan 17 15:46:40.848982 aaa:AAA_REQ_RESPONSE_NOT_NEEDEDの設定

2018 Jan 17 15:46:40.848992 aaa:aaa_req_process:applnからの一般的なAAA要求：デフォルトのappln_subtype:default

2018 Jan 17 15:46:40.849002 aaa:try_next_aaa_method

2018 Jan 17 15:46:40.849022 aaa:デフォルトで設定されている方法はありません

2018 Jan 17 15:46:40.849032 aaa:この要求に使用できる構成がありません

2018 Jan 17 15:46:40.849043 aaa:try_fallback_method

2018 Jan 17 15:46:40.849053 aaa:handle_req_using_method

2018 Jan 17 15:46:40.849063 aaa:local_method_handler

2018 Jan 17 15:46:40.849073 aaa:aaa_local_accounting_msg

2018 Jan 17 15:46:40.849085 aaa:update:::added user:fxosadmin to role:admin

認証に失敗すると、次の出力が表示されます。

2018 Jan 17 15:46:17.836271 aaa:aaa_req_processを使用します。session no 0

2018 Jan 17 15:46:17.836616 aaa:aaa_req_process:applnからの一般的なAAA要求：login appln_subtype:default

2018 Jan 17 15:46:17.837063 aaa:try_next_aaa_method

2018 Jan 17 15:46:17.837416 aaa:設定されたメソッドの総数は1、試行される現在のインデックスは0

2018 Jan 17 15:46:17.837766 aaa:handle_req_using_method

2018 Jan 17 15:46:17.838103 aaa:AAA_METHOD_SERVER_GROUP

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

2018 Jan 17 15:46:17.838826 aaa:この関数に渡されるsg_protocolの使用

2018 Jan 17 15:46:17.839167 aaa:TACACSサービスへの要求の送信

2018 Jan 17 15:46:17.840225 aaa:構成されたメソッドグループが成功しました

2018 Jan 17 15:46:18.043710 aaa:is_aaa_resp_status_success status = 2

2018 Jan 17 15:46:18.044048 aaa:is_aaa_resp_status_successはTRUEです

2018 Jan 17 15:46:18.044395 aaa:aaa_send_client_responseを使用します。session->flags=21. aaa_resp->flags=0.

2018 Jan 17 15:46:18.044733 aaa:AAA_REQ_FLAG_NORMAL

2018 Jan 17 15:46:18.045096 aaa:mts_send_response成功

2018 Jan 17 15:46:18.045677 aaa:aaa_cleanup_session

2018 Jan 17 15:46:18.045689 aaa:要求メッセージのmts_drop

2018 Jan 17 15:46:18.045699 aaa:aaa_reqは解放される必要があります。

2018 Jan 17 15:46:18.045715 aaa:aaa_process_fd_set

2018 Jan 17 15:46:18.045722 aaa:aaa_process_fd_set:aaa_qのmtscallback

2018 Jan 17 15:46:18.045732 aaa:aaa_enable_info_config:GET_REQ for aaa loginエラーメッセージ

2018 Jan 17 15:46:18.045738 aaa:設定操作の戻り値を取得しました：不明なセキュリティ項目

関連情報

TACACS/RADIUS認証が有効な場合、FX-OS CLIでEthanalyzerコマンドを実行すると、パスワードの入力を求めるプロンプトが表示されます。この動作はバグが原因です。

Bug ID: CSCvg87518