Sistema operacional Firepower eXtensible (FXOS) 2.2: Autenticação/autorização do chassi para gerenciamento remoto com ISE usando TACACS+

Contents

Introduction

Este documento descreve como configurar a autenticação e autorização TACACS+ para o chassi do Firepower eXtensible Operating System (FXOS) através do Identity Services Engine (ISE).

O chassi FXOS inclui as seguintes funções de usuário:

- Administrador - Acesso completo de leitura e gravação a todo o sistema. A conta admin padrão recebe essa função por padrão e não pode ser alterada.
- Somente leitura - Acesso somente leitura à configuração do sistema sem privilégios para modificar o estado do sistema.
- Operações - Acesso de leitura e gravação à configuração do NTP, configuração do Smart Call Home para Smart Licensing e registros do sistema, incluindo servidores de syslog e falhas. Leia o acesso ao restante do sistema.
- AAA - acesso de leitura e gravação a usuários, funções e configuração de AAA. Leia o acesso ao restante do sistema.

Através da CLI, isso pode ser visto da seguinte maneira:

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

Função:

Nome da função Priv

—

aaa aaa

admin admin

operações operacionais

somente leitura

Contribuído por Tony Remirez, José Soto, engenheiros do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do Firepower eXtensible Operating System (FXOS)
- Conhecimento da configuração do ISE
- A licença TACACS+ Device Administration é necessária no ISE

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Firepower 4120 Security Appliance versão 2.2
- Cisco Identity Services Engine 2.2.0.470 virtual

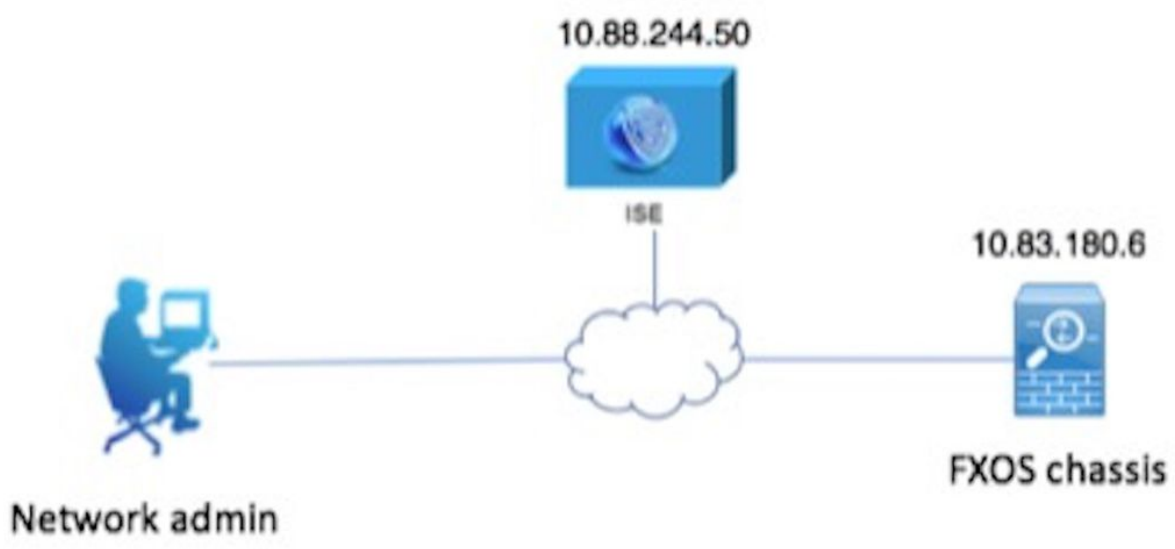
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

O objetivo da configuração é:

- Autentique os usuários que fazem login na GUI baseada na Web e no SSH do FXOS por meio do ISE
- Autorize os usuários a fazer login na GUI baseada na Web e no SSH do FXOS de acordo com sua respectiva função de usuário por meio do ISE.
- Verificar a operação adequada de autenticação e autorização no FXOS por meio do ISE

Diagrama de Rede



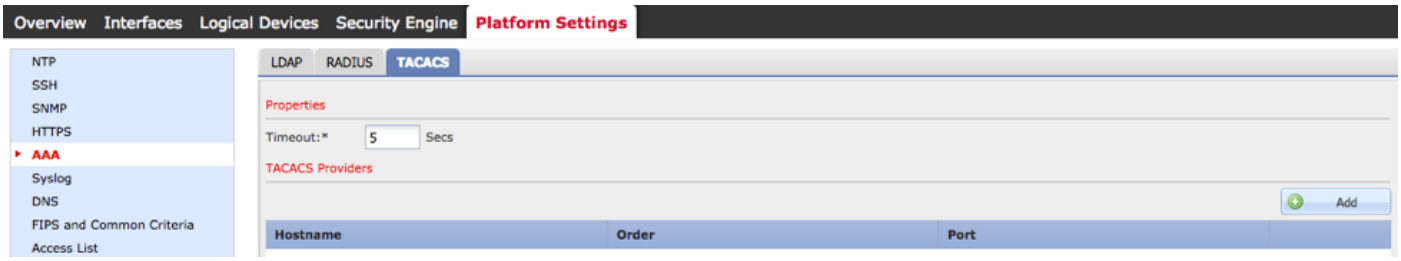
Configurações

Configurando o chassi FXOS

Criando um provedor TACACS+

Etapa 1. Navegue até **Configurações da plataforma > AAA.**

Etapa 2. Clique na guia **TACACS**.

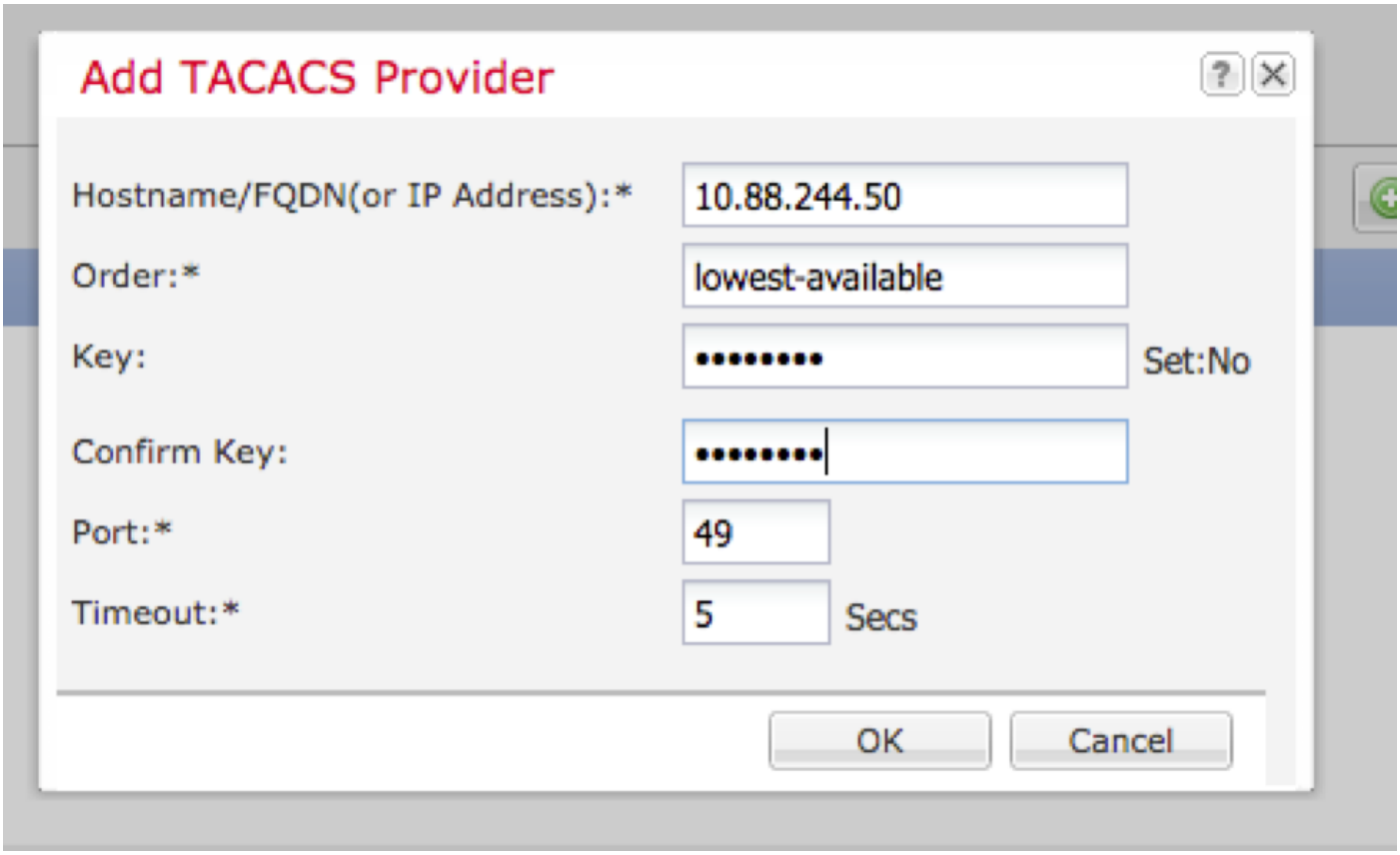


Etapa 3. Para cada provedor TACACS+ que você deseja adicionar (até 16 provedores).

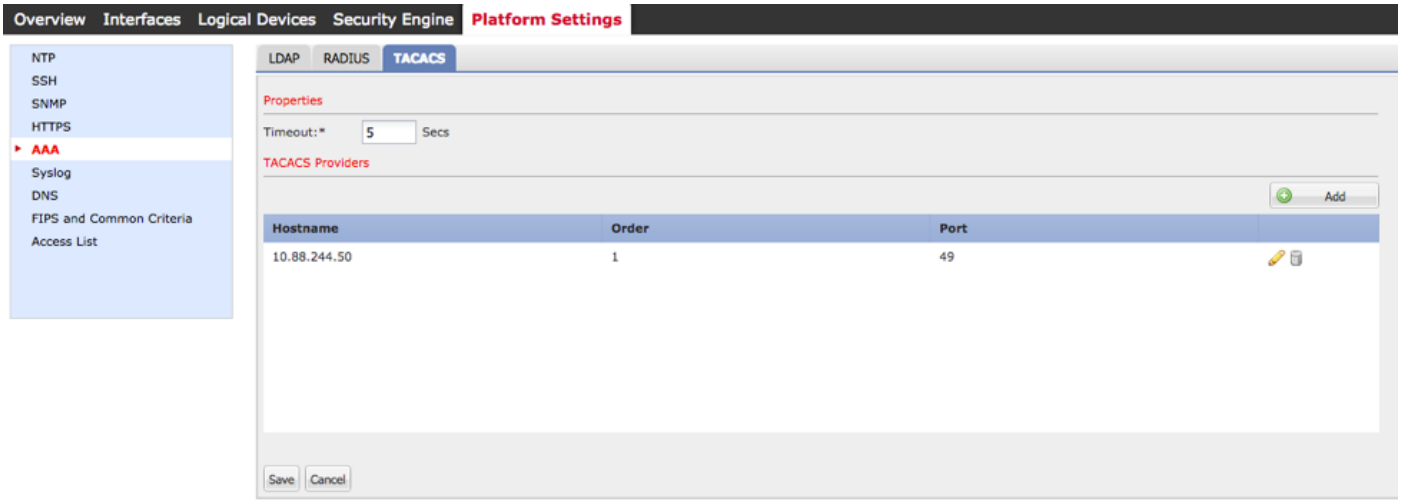
3.1. Na área TACACS Providers, clique em **Add.**

3.2. Quando a caixa de diálogo Add TACACS Provider for aberta, insira os valores necessários.

3.3. Clique em **OK** para fechar a caixa de diálogo Adicionar Provedor TACACS.

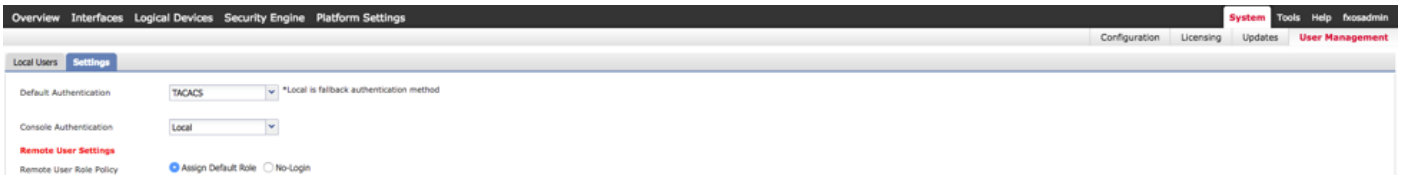


Etapa 4. Click **Save**.



Etapa 5. Navegue até **System > User Management > Settings**.

Etapa 6. Em Autenticação padrão, escolha **TACACS**.



Criando um provedor TACACS+ usando CLI

Etapa 1. Para habilitar a autenticação TACACS, execute os seguintes comandos.

segurança de escopo fpr4120-TAC-A#

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

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

Etapa 2. Use o comando **show detail** para verificar a configuração.

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

Autenticação padrão:

Domínio administrativo: **TACACS**

Domínio operacional: **TACACS**

Período de atualização da sessão da Web (em segundos): 600

Tempo limite da sessão (em segundos) para sessões web, ssh, telnet: 600

Tempo limite da sessão absoluta (em segundos) para sessões web, ssh, telnet: 3600

Tempo limite da sessão do console serial (em segundos): 600

Tempo limite da sessão absoluta do console serial (em segundos): 3600

Grupo de servidores de Autenticação do Administrador:

Grupo de servidores de Autenticação Operacional:

Uso do segundo fator: No

Etapa 3. Para configurar os parâmetros do servidor TACACS, execute os seguintes comandos.

segurança de escopo fpr4120-TAC-A#

fpr4120-TAC-A /segurança # **táticas de escopo**

fpr4120-TAC-A /security/tacacs # **entre no servidor 10.88.244.50**

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

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

Digite a chave: ******

Confirme a chave: ******

Etapa 4. Use o comando **show detail** para verificar a configuração.

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

Servidor TACACS+:

Nome do host, FQDN ou endereço IP: 10.88.244.50

Descr:

Pedido: 1

Porta: 49

Chave: ****

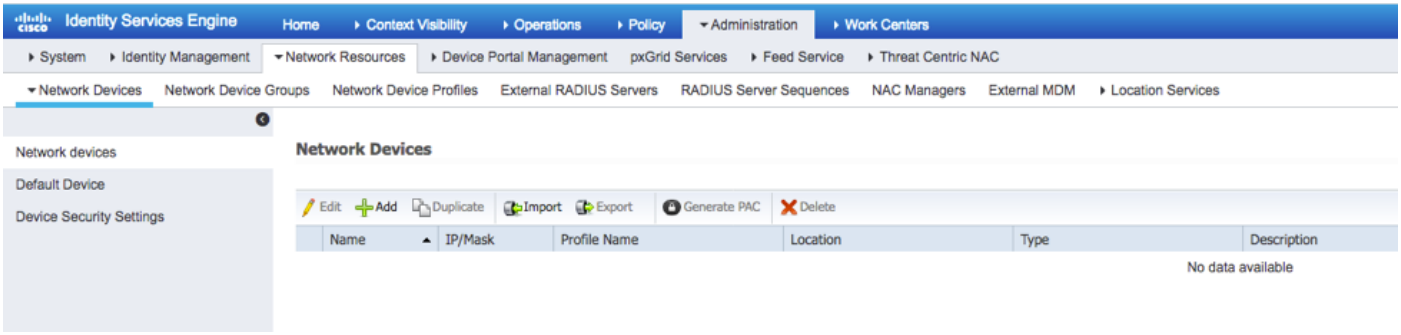
tempo limite: 5

Configuração do servidor ISE

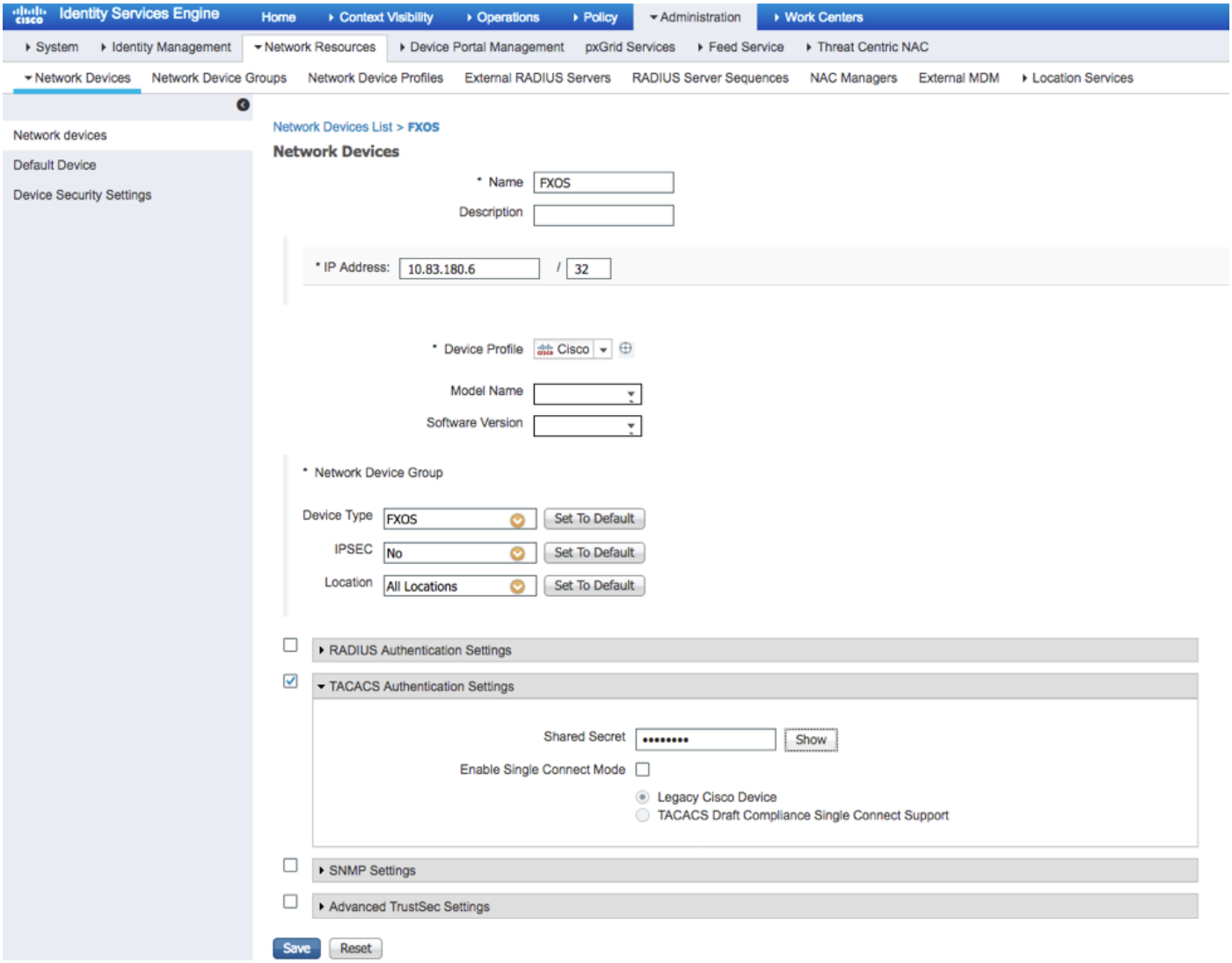
Adicionando o FXOS como um recurso de rede

Etapa 1. Navegue até **Administration > Network Resources > Network Devices**.

Etapa 2. Clique em Add.



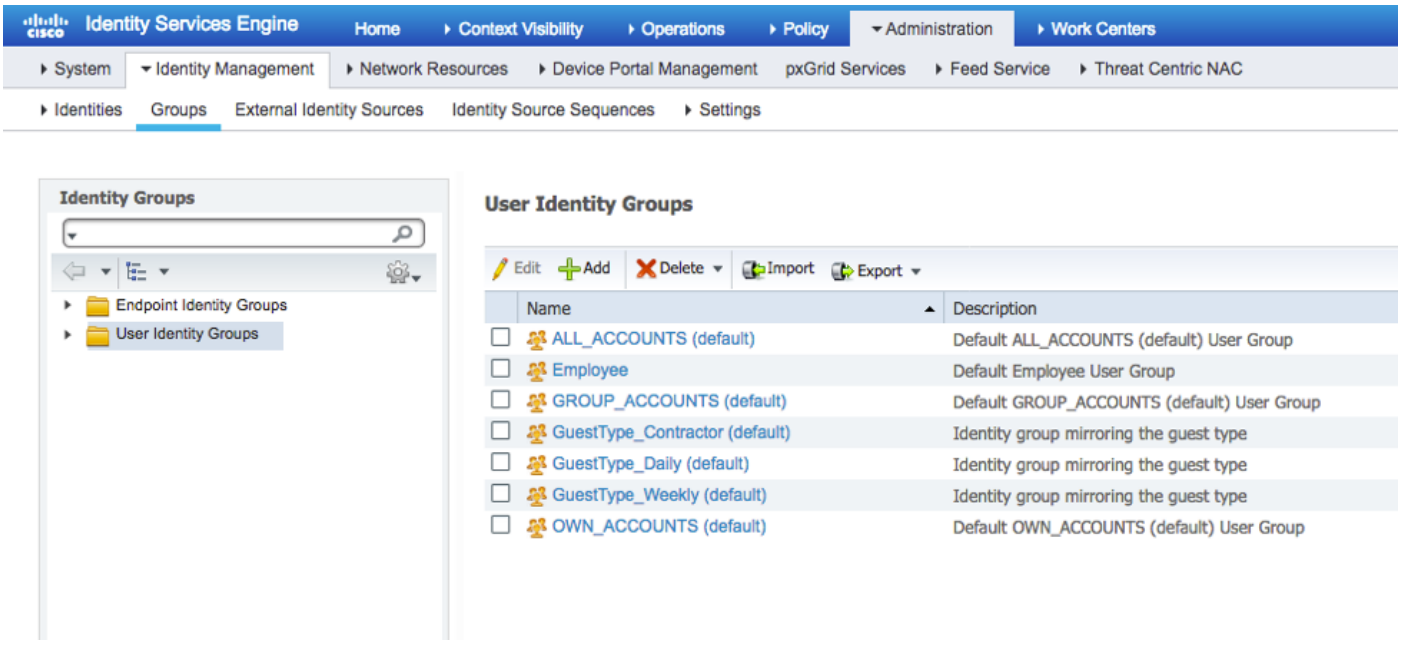
Etapa 3. Insira os valores necessários (Nome, Endereço IP, Tipo de dispositivo e Habilitar TACACS+ e adicione a CHAVE), clique em **Enviar.**



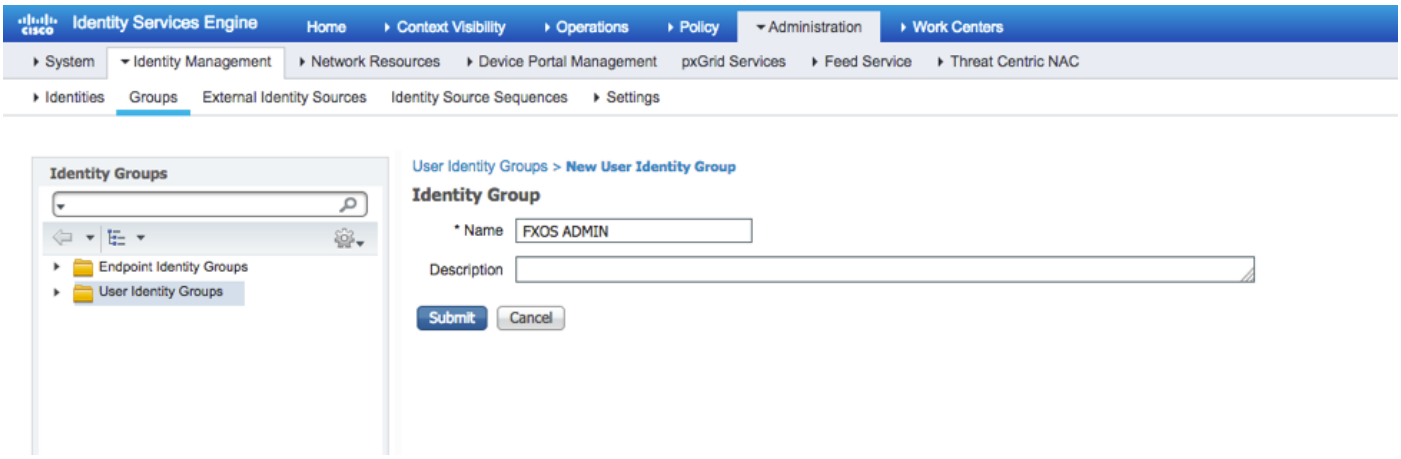
Criando grupos de identidade e usuários

Etapa 1. Navegue até **Administration > Identity Management > Groups > User Identity Groups.**

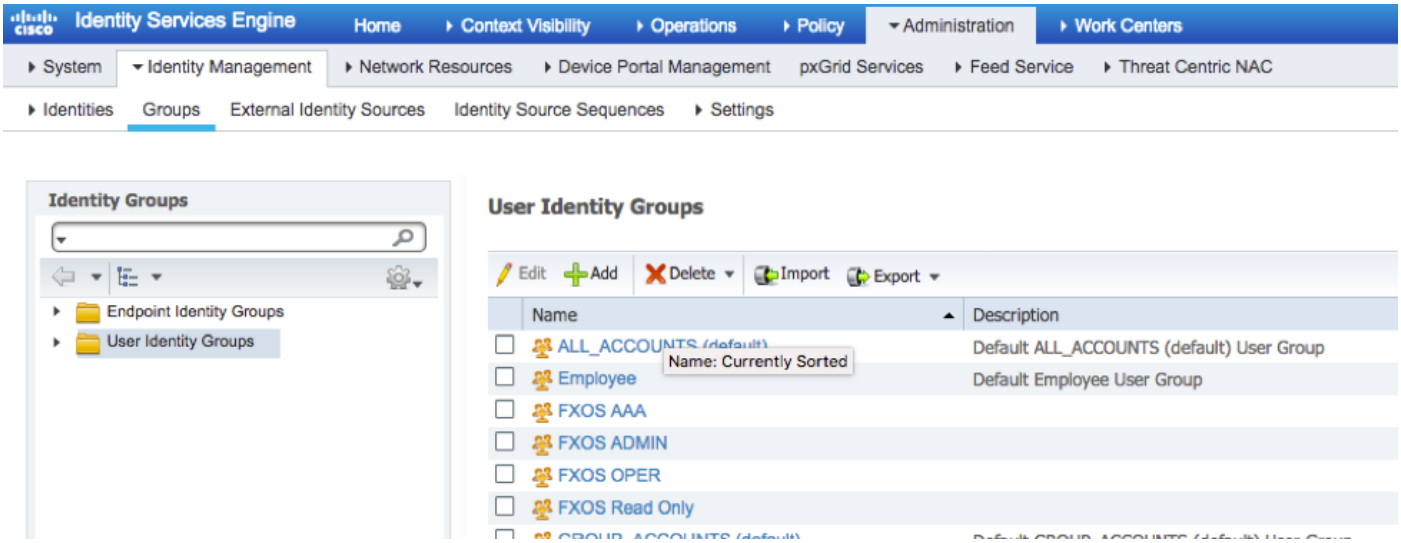
Etapa 2. Clique em Add.



Etapa 3. Insira o valor para Nome e clique em **Enviar.**

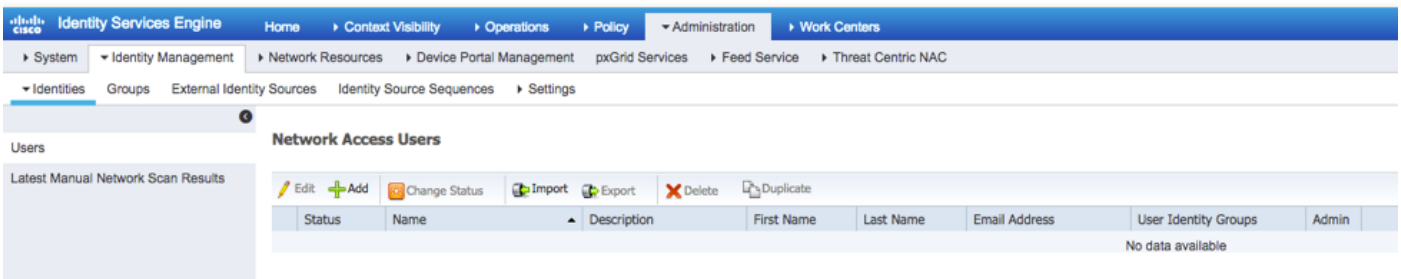


Etapa 4. Repita a etapa 3 para todas as funções de usuário necessárias.

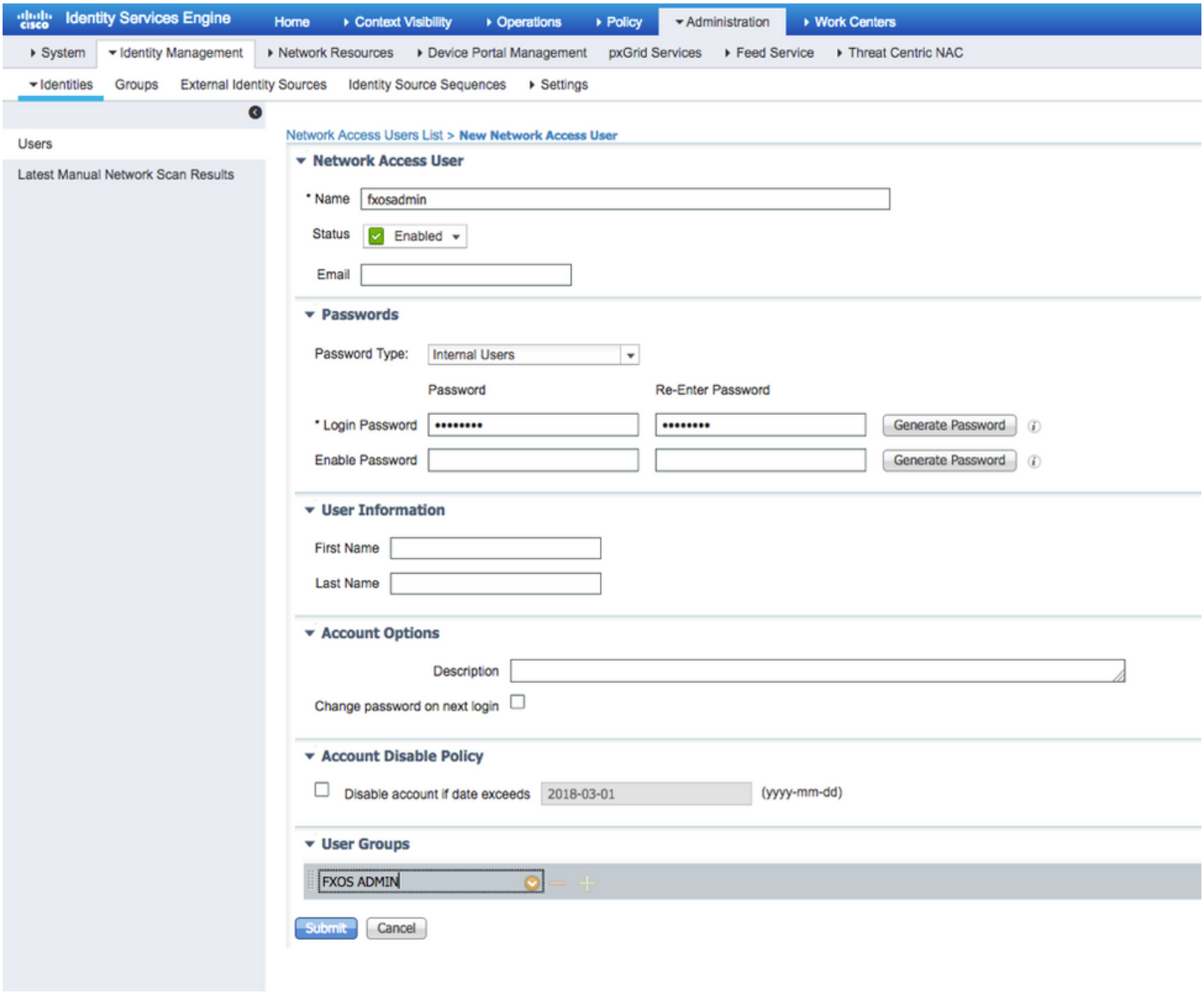


Etapa 5. Navegue até **Administration > Identity Management > Identity > Users.**

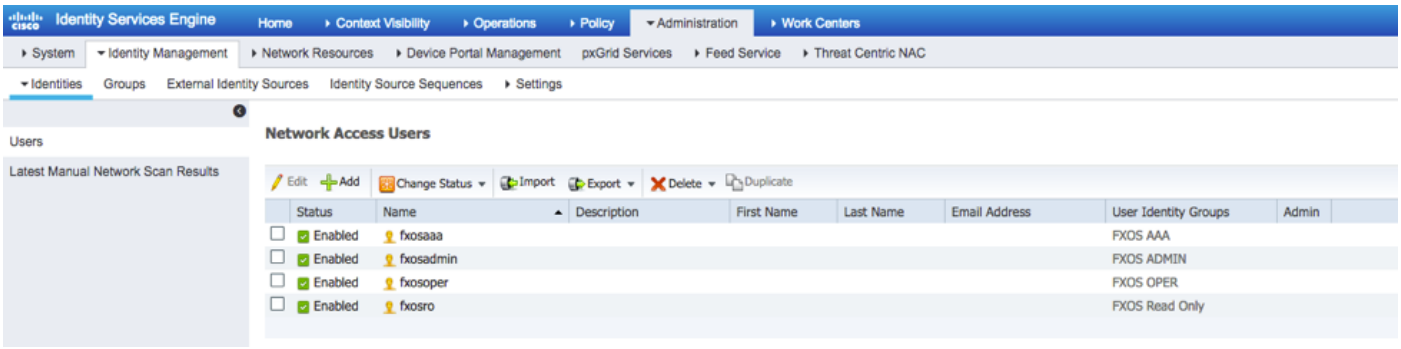
Etapa 6. Clique em Add.



Passo 7. Insira os valores necessários (Nome, Grupo de usuários, Senha).

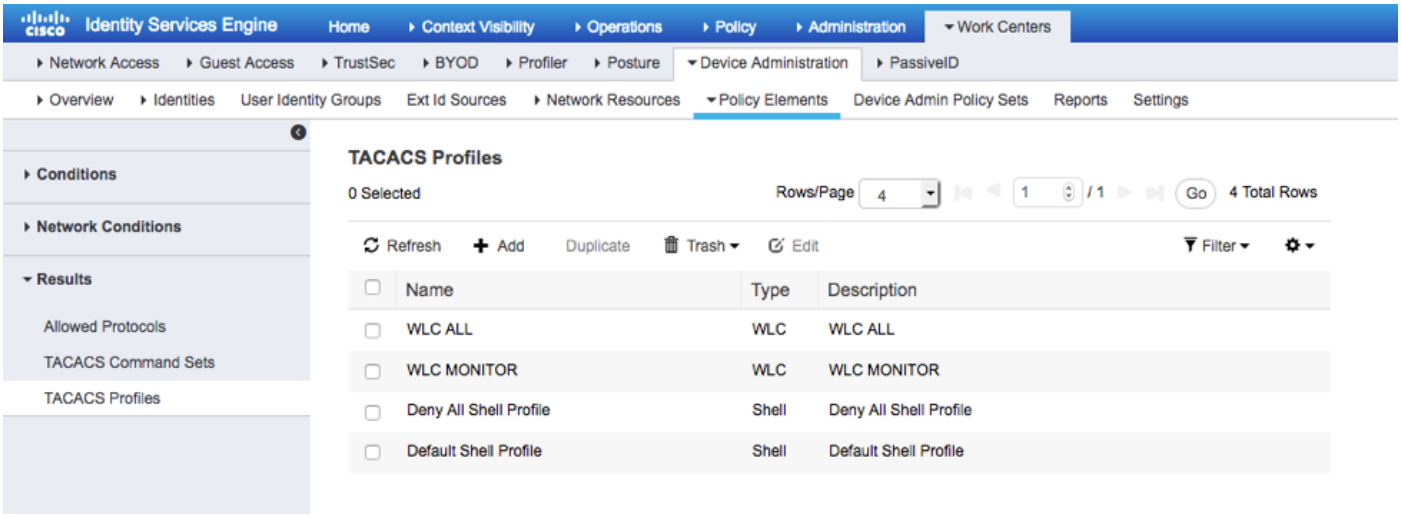


Etapa 8. Repita a etapa 6 para todos os usuários necessários.



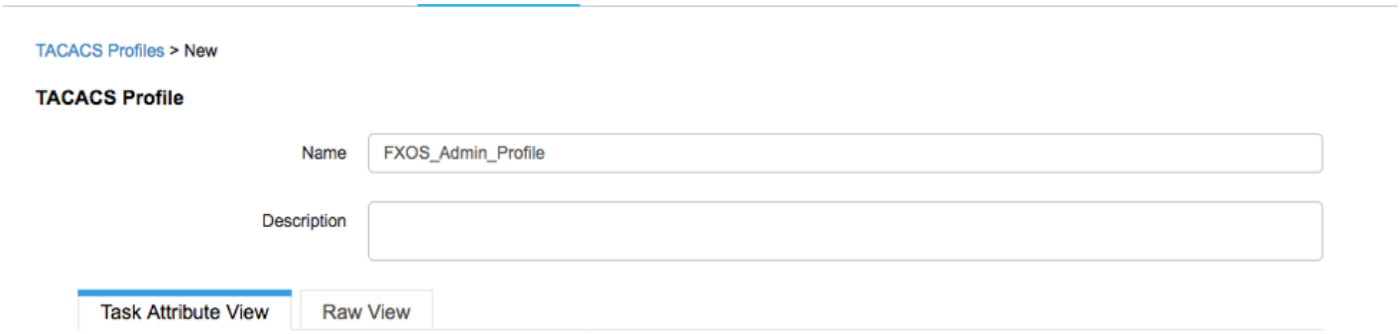
Criando o perfil de shell para cada função de usuário

Etapa 1. Navegue até **Centros de trabalho > Administração do dispositivo > Elementos de política > Resultados > Perfis TACACS** e clique em **+ADD.**



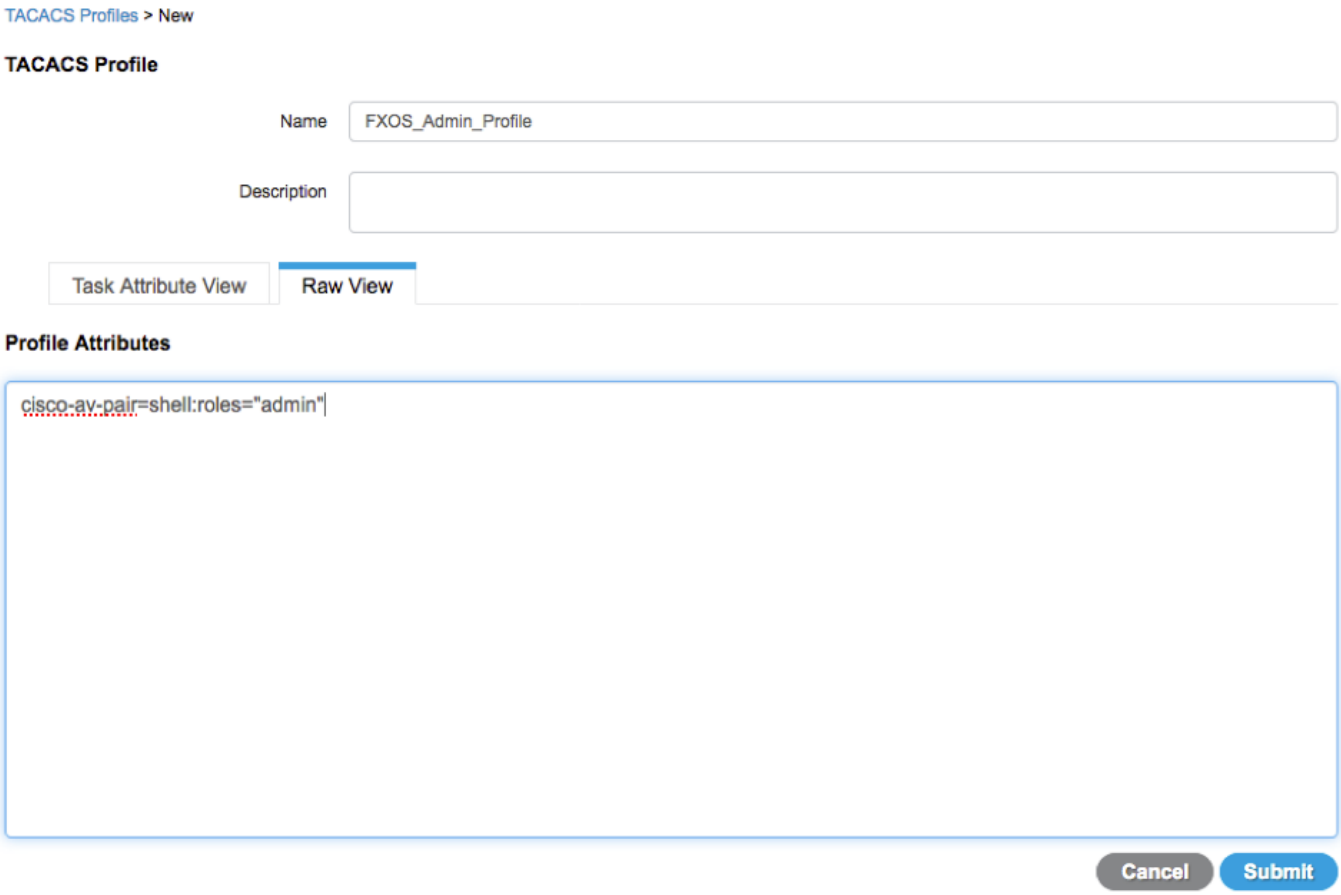
Etapa 2. Insira os valores necessários para o perfil TACACS

2.1. Digite o nome.

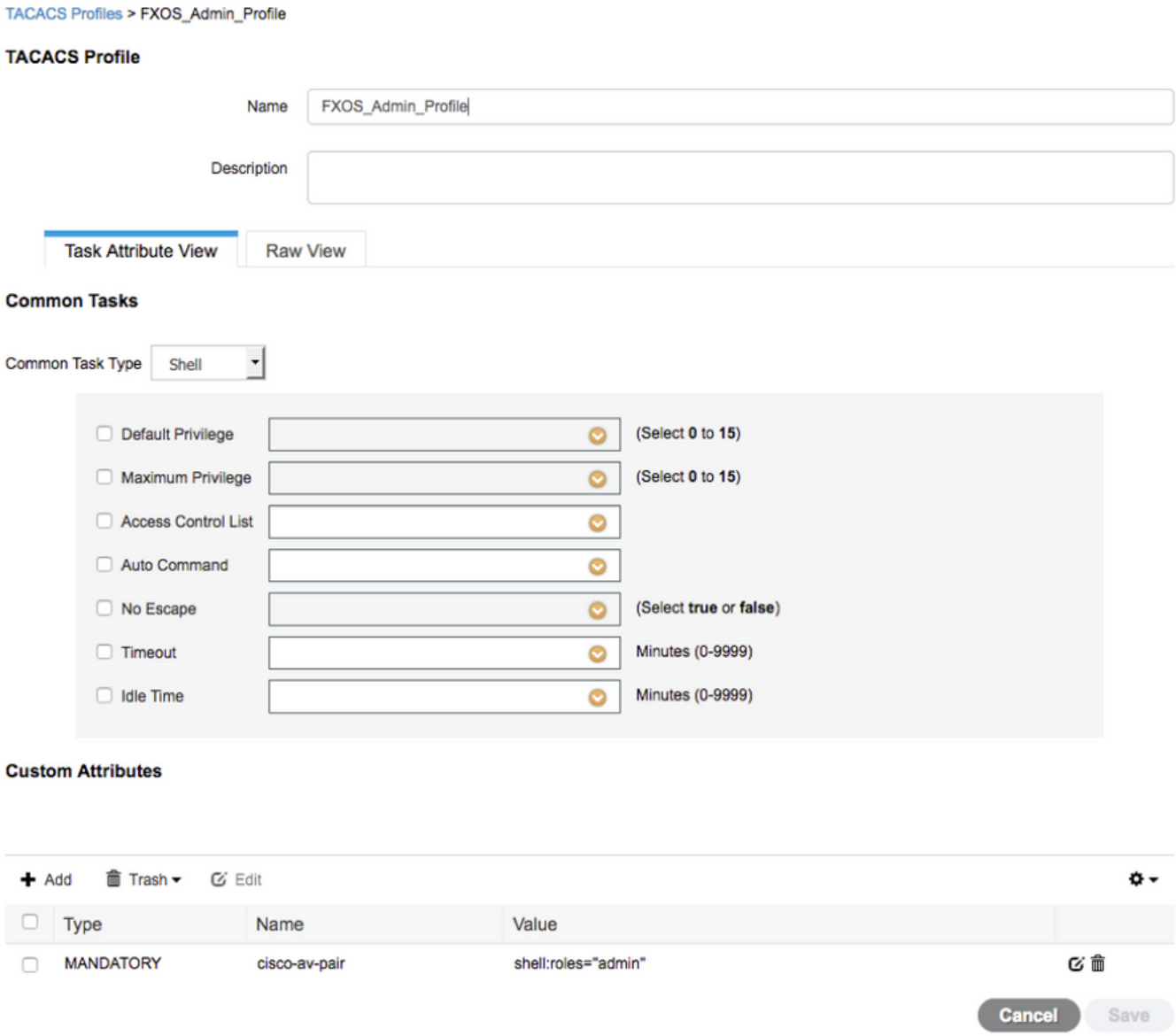


2.2. Na guia **RAW View**, configure o CISCO-AV-PAIR a seguir.

cisco-av-pair=shell:funções="admin"



2.3. Clique em Submit.

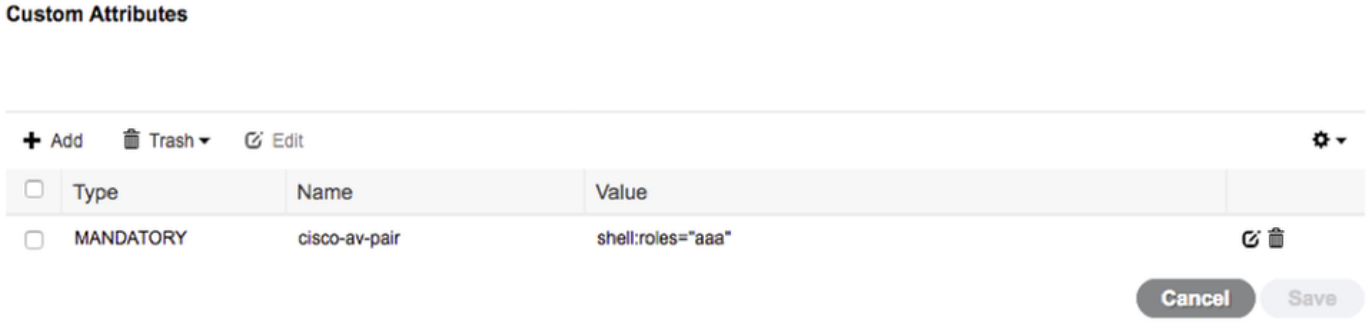


Etapa 3. Repita a etapa 2 para as funções de usuário restantes usando os seguintes pares Cisco-AV.

cisco-av-pair=shell:funções="aaa"

cisco-av-pair=shell:funções="operações"

cisco-av-pair=shell:funções="somente leitura"



Custom Attributes

+ Add | Trash | Edit

Type	Name	Value
MANDATORY	cisco-av-pair	shell:roles="operations"

Custom Attributes

+ Add | Trash | Edit

Type	Name	Value
MANDATORY	cisco-av-pair	shell:roles="read-only"

TACACS Profiles

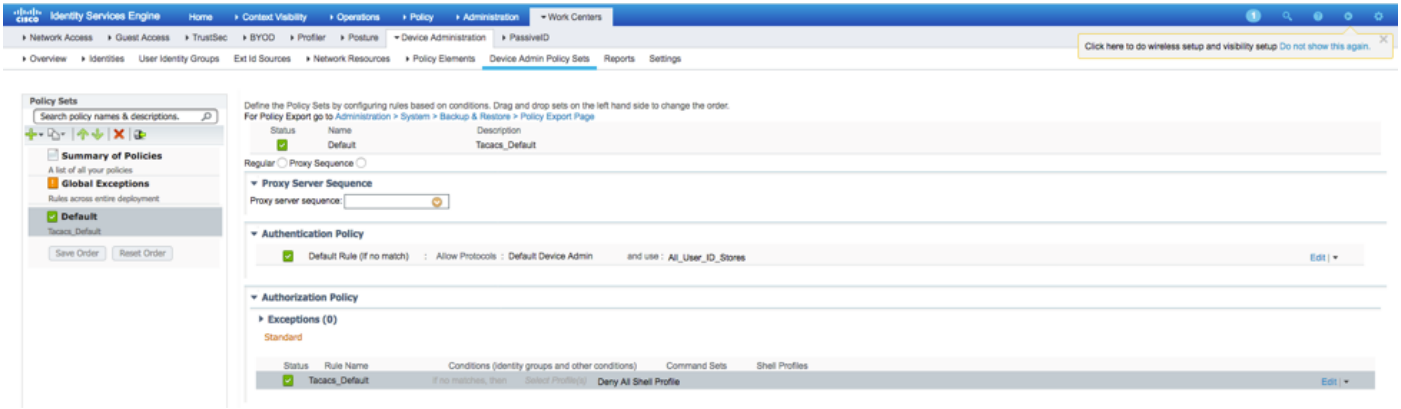
0 Selected | Rows/Page 8 | 1 / 1 | Go | 8 Total Rows

Refresh | + Add | Duplicate | Trash | Edit | Filter

Name	Type	Description
WLC ALL	WLC	WLC ALL
WLC MONITOR	WLC	WLC MONITOR
Deny All Shell Profile	Shell	Deny All Shell Profile
Default Shell Profile	Shell	Default Shell Profile
FXOS_Admin_Profile	Shell	
FXOS_AAA_Shell	Shell	
FXOS_Operations_Shell	Shell	
FXOS_ReadOnly_Shell	Shell	

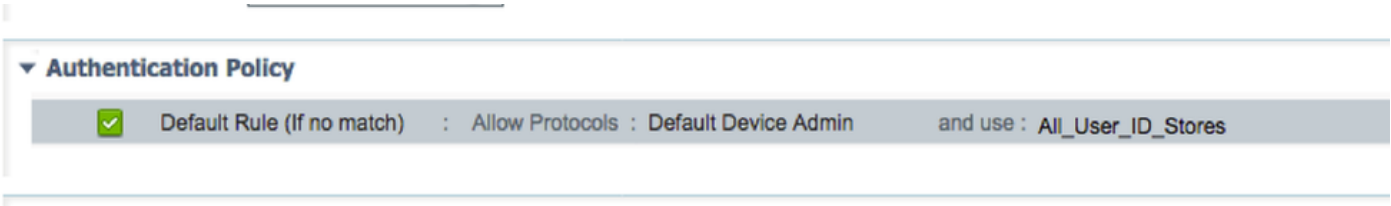
Criando a política de autorização TACACS

Etapa 1. Navegue até **Centros de trabalho > Administração do dispositivo > Conjuntos de políticas de administração do dispositivo.**



Etapa 2. Certifique-se de que a Política de Autenticação aponte para o banco de dados de

Usuários Internos ou para o Repositório de Identidades necessário.



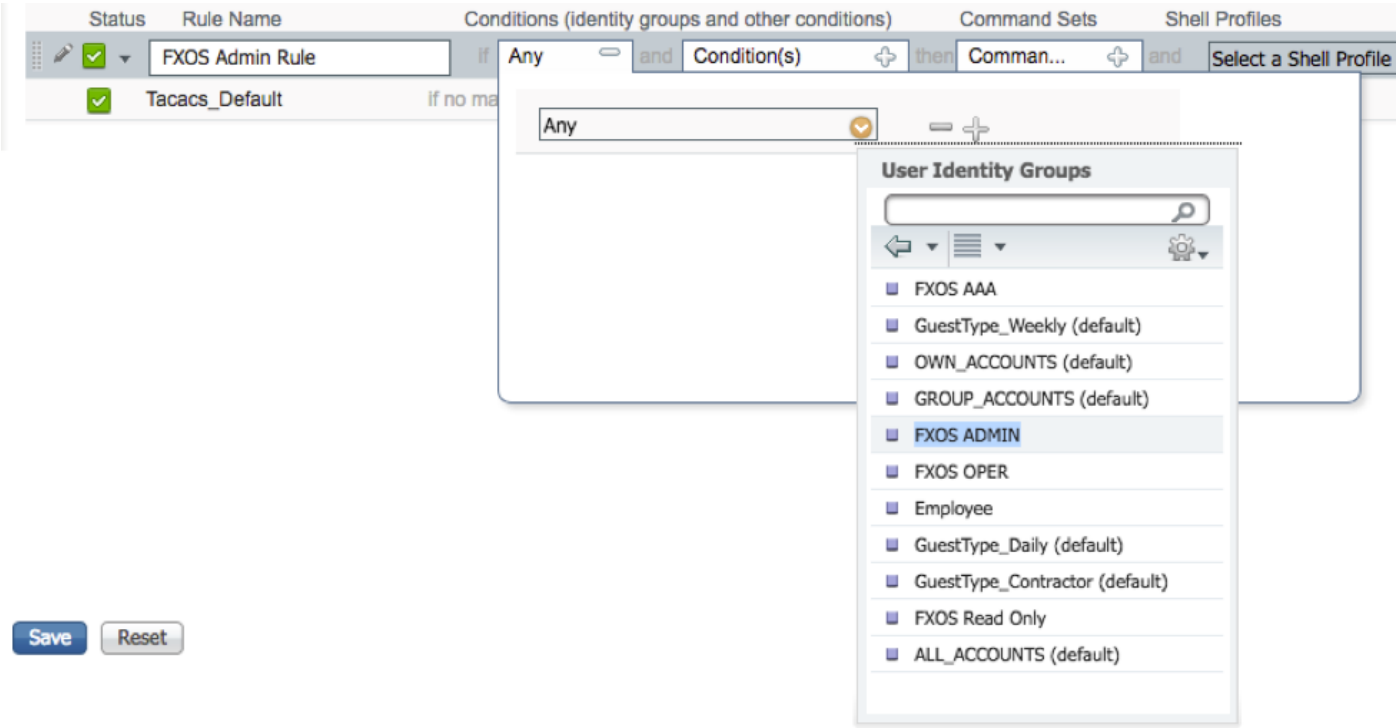
Etapa 3. Clique na seta ao final da diretiva de autorização padrão e clique em inserir regra acima.

Etapa 4. Insira os valores da regra com os parâmetros necessários:

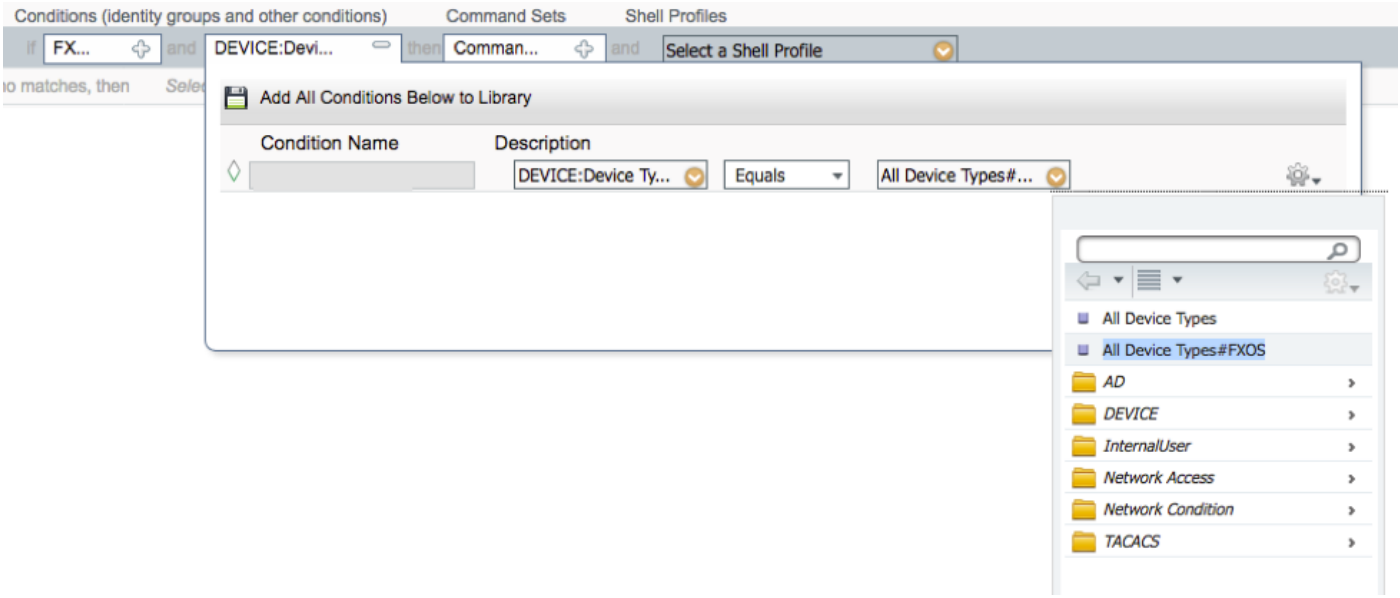
4.1. Nome da regra: Regra de administração FXOS.

4.2. Condições.

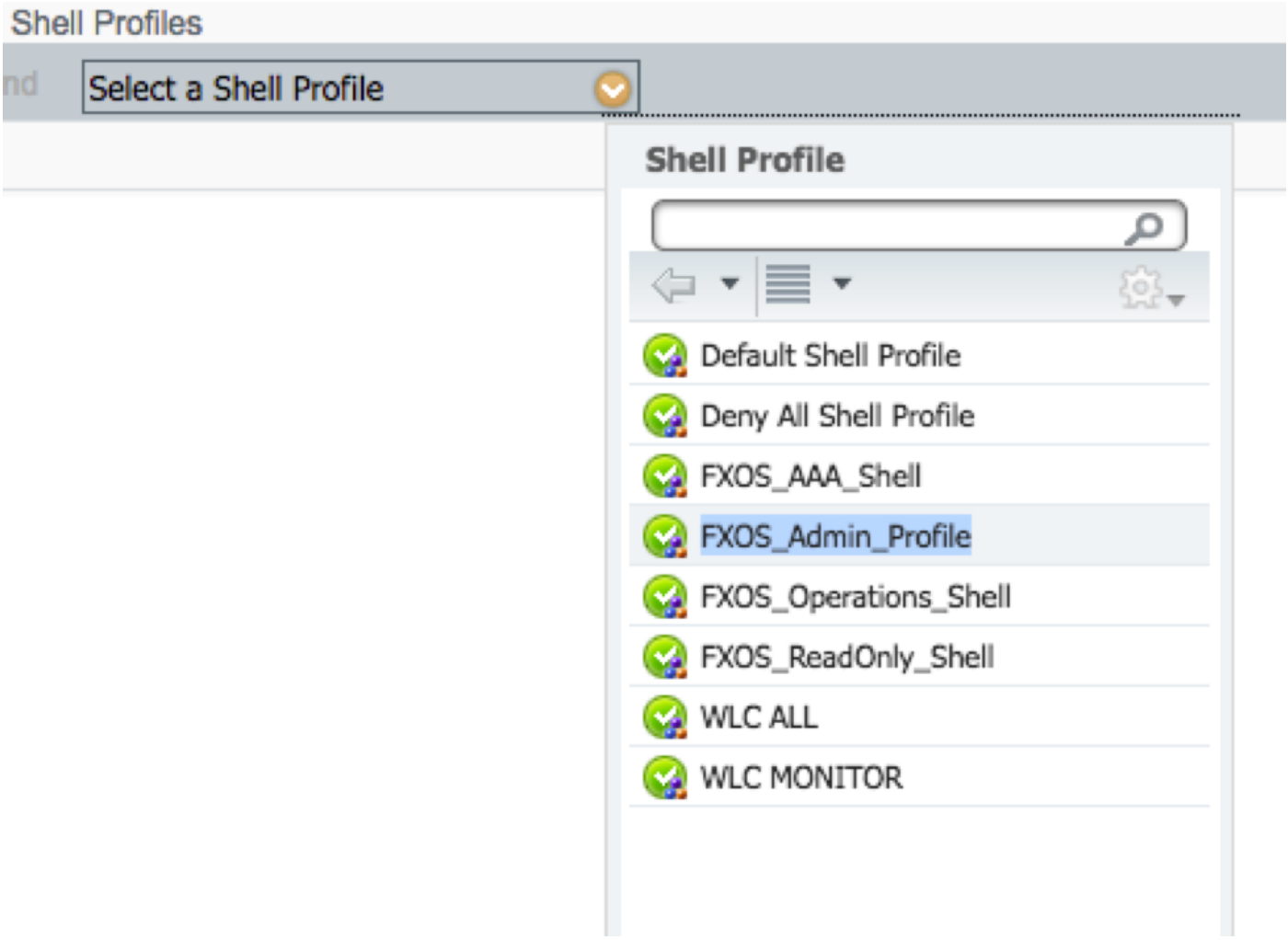
Se: O grupo de identidade do usuário é ADMIN FXOS



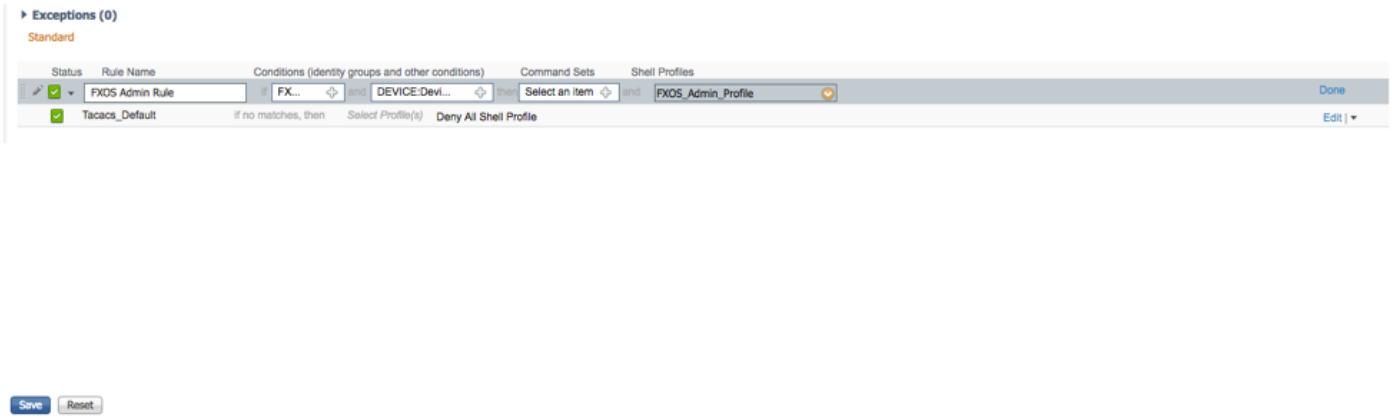
E dispositivo: Tipo de dispositivo é igual a todos os tipos de dispositivo #FXOS



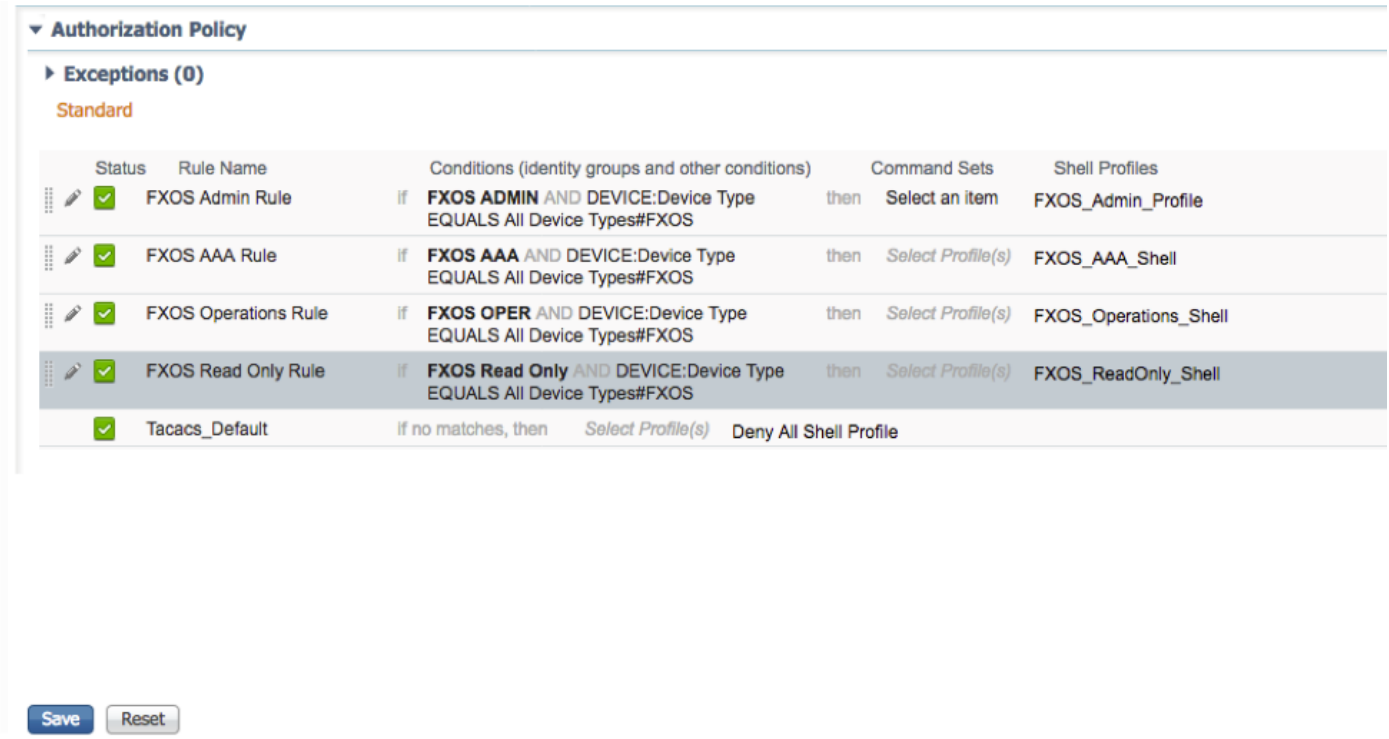
Perfil da Shell: FXOS_Admin_Profile



Etapa 5. Clique em Concluído.



Etapa 6. Repita as etapas 3 e 4 para as funções de usuário restantes e, quando terminar, clique em **SALVAR**.



Verificar

Agora você pode testar cada usuário e verificar a função de usuário atribuída.

Verificação de chassi FXOS

1. Faça Telnet ou SSH para o chassi FXOS e faça login usando qualquer um dos usuários criados no ISE.

Nome de usuário: fxosadmin

Senha:

fpr4120-TAC-A# **segurança de escopo**

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

Arquivo de usuário remoto:

Descrição:

Funções de usuário:

Nome: **aaa**

Nome: **somente leitura**

Usuário remoto **fxosadmin**:

Descrição:

Funções de usuário:

Nome: **admin**

Nome: **somente leitura**

Usuário remoto **operacional**:

Descrição:

Funções de usuário:

Nome: **operações**

Nome: **somente leitura**

Fxosor do usuário remoto:

Descrição:

Funções de usuário:

Nome: **somente leitura**

Dependendo do nome de usuário inserido, a cli do chassi do FXOS exibirá apenas os comandos autorizados para a função de usuário atribuída.

Função de Usuário Admin.

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

Reconhecer

clear-user-sessions Clear User Sessions

criar objetos gerenciados

excluir excluir objetos gerenciados

desabilitar desabilita serviços

enable Habilita serviços

inserir um objeto gerenciado

escopo Altera o modo atual

definir valores de propriedade

show system information

terminar sessões cimc ativas

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

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

fpr4120-TAC-A (fxos)#

Função de usuário somente leitura.

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

escopo Altera o modo atual

definir valores de propriedade

show system information

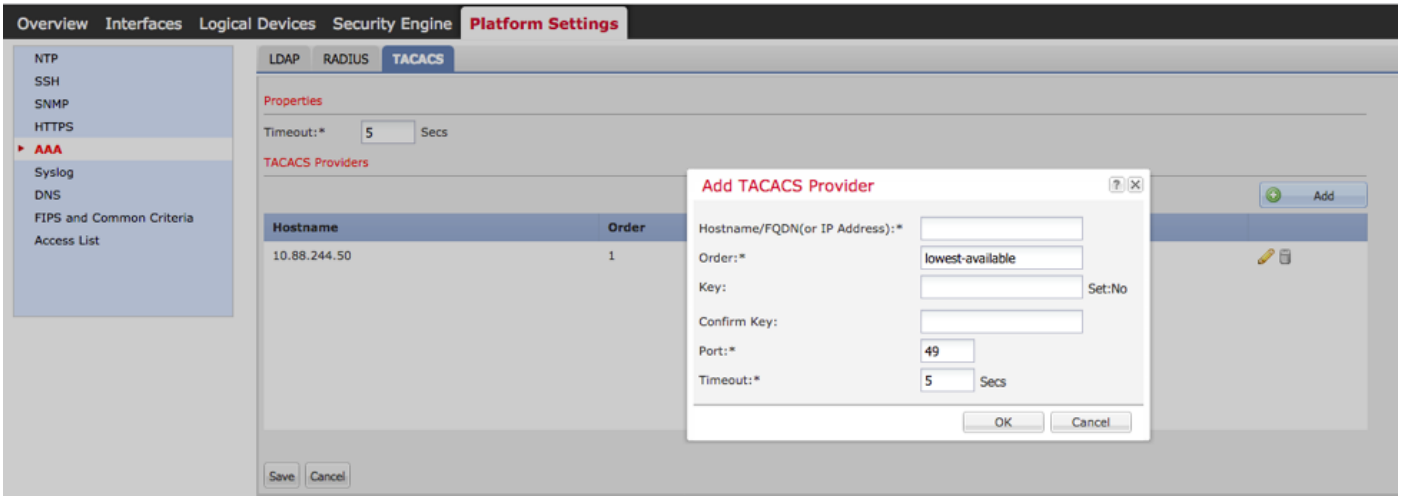
fpr4120-TAC-A# **connect fxos**

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

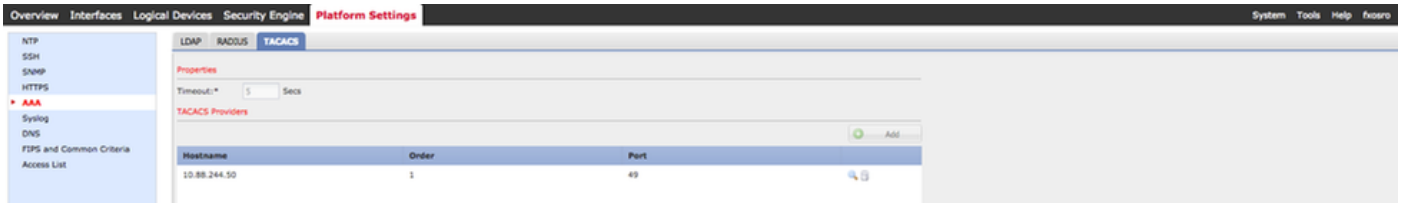
% Permissão negada para a função

2. Navegue até o endereço IP do chassi FXOS e faça login usando qualquer um dos usuários criados no ISE.

Função de Usuário Admin.



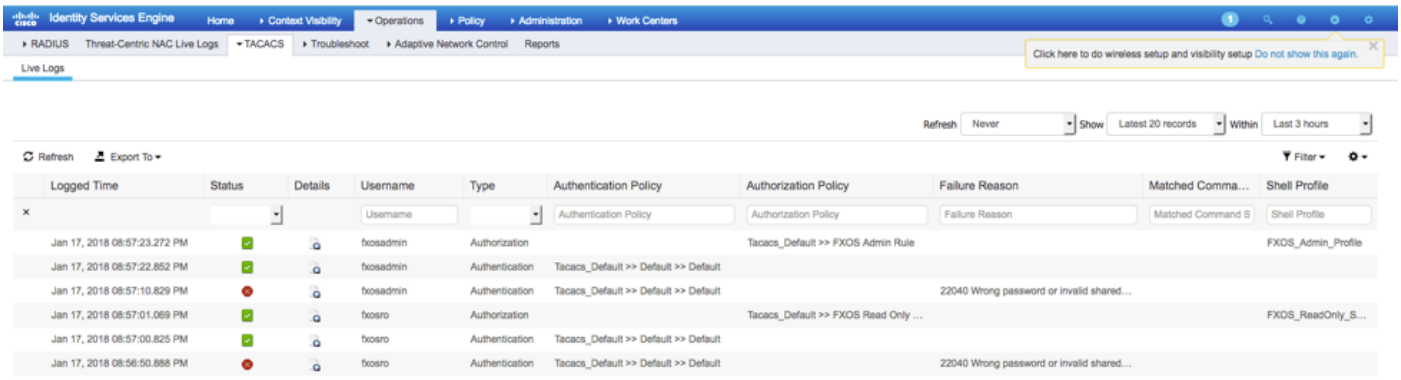
Função de usuário somente leitura.



Note: Observe que o botão **ADD** está acinzentado.

Verificação do ISE 2.0

1. Navegue até **Operations > TACACS Livelog.** Você deve ser capaz de ver tentativas bem-sucedidas e com falha.



Troubleshoot

Para depurar a autenticação e a autorização AAA, execute os seguintes comandos na cli do FXOS.

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

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

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

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

fpr4120-TAC-A (fxos)#term mon

Após uma tentativa de autenticação bem-sucedida, você verá a seguinte saída.

2018 Jan 17 15:46:40.305247 aaa: aaa_req_process para autenticação. session no 0

2018 Jan 17 15:46:40.305262 aaa: aaa_req_process: Solicitação geral de AAA do appln: login appln_subtype: padrão

2018 Jan 17 15:46:40.305271 aaa: try_next_aaa_method

2018 Jan 17 15:46:40.305285 aaa: total de métodos configurados é 1, índice atual a ser tentado é 0

2018 Jan 17 15:46:40.305294 aaa: fp_req_using_method

2018 Jan 17 15:46:40.305301 aaa: AAA_METOD_SERVER_GROUP

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

2018 Jan 17 15:46:40.305315 aaa: Usando sg_protocol que é passado para esta função

2018 Jan 17 15:46:40.305324 aaa: Enviando solicitação para o serviço TACACS

2018 Jan 17 15:46:40.305384 aaa: Grupo de métodos configurado com êxito

2018 Jan 17 15:46:40.554631 aaa: aaa_process_fd_set

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

2018 Jan 17 15:46:40.555817 aaa: mts_message_response_handler: uma resposta mts

2018 Jan 17 15:46:40.556387 aaa: prot_daemon_reponse_handler

2018 Jan 17 15:46:40.557042 aaa: sessão: 0x8dfd68c removido da tabela de sessão 0

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

2018 Jan 17 15:46:40.557066 aaa: is_aaa_resp_status_successful é TRUE

2018 Jan 17 15:46:40.557075 aaa: aaa_send_client_response para autenticação. 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 Bem-sucedido

2018 Jan 17 15:46:40.557364 aaa: aaa_req_process para autorização. session no 0

2018 Jan 17 15:46:40.557378 aaa: aaa_req_process chamado com o contexto do 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 = (nulo)

2018 Jan 17 15:46:40.557401 aaa: Usando sg_protocol que é passado para esta função

2018 Jan 17 15:46:40.557408 aaa: solicitação AAA baseada em contexto ou direcionada(exceção: não uma solicitação de retransmissão). Não receberá cópia da solicitação aaa

2018 Jan 17 15:46:40.557415 aaa: Enviando solicitação para o serviço TACACS

2018 Jan 17 15:46:40.801732 aaa: aaa_send_client_response para autorização. session->flags=9. aaa_resp->flags=0.

2018 Jan 17 15:46:40.801740 aaa: AAA_REQ_FLAG_NORMAL

2018 Jan 17 15:46:40.801761 aaa: mts_send_response Bem-sucedido

2018 Jan 17 15:46:40.848932 aaa: CÓDIGO ANTIGO: accounting_mid_update

2018 Jan 17 15:46:40.848943 aaa: aaa_create_local_acct_req: user=, session_id=, log=adicionou user:fxosadmin à função:admin

2018 Jan 17 15:46:40.848963 aaa: aaa_req_process para contabilidade. session no 0

2018 Jan 17 15:46:40.848972 aaa: A referência de solicitação MTS é NULL. solicitação LOCAL

2018 Jan 17 15:46:40.848982 aaa: Definindo AAA_REQ_RESPONSE_NOT_NEEDED

2018 Jan 17 15:46:40.848992 aaa: aaa_req_process: Solicitação geral de AAA do appln: appln_subtype padrão: padrão

2018 Jan 17 15:46:40.849002 aaa: try_next_aaa_method

2018 Jan 17 15:46:40.849022 aaa: nenhum método configurado para o padrão

2018 Jan 17 15:46:40.849032 aaa: nenhuma configuração disponível para esta solicitação

2018 Jan 17 15:46:40.849043 aaa: try_fallback_method

2018 Jan 17 15:46:40.849053 aaa: fp_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: atualização:::usuário adicionado:fxosadmin à função:admin

Após uma tentativa de autenticação com falha, você verá a seguinte saída.

2018 Jan 17 15:46:17.836271 aaa: aaa_req_process para autenticação. session no 0

2018 Jan 17 15:46:17.836616 aaa: aaa_req_process: Solicitação geral de AAA do appln: login appln_subtype: padrão

2018 Jan 17 15:46:17.837063 aaa: try_next_aaa_method

2018 Jan 17 15:46:17.837416 aaa: total de métodos configurados é 1, índice atual a ser tentado é 0

2018 Jan 17 15:46:17.837766 aaa: fp_req_using_method

2018 Jan 17 15:46:17.838103 aaa: AAA_METOD_SERVER_GROUP

2018 Jan 17 15:46:17.838477 aaa: aaa_sg_method_handler group = tacacs

2018 Jan 17 15:46:17.838826 aaa: Usando sg_protocol que é passado para esta função

2018 Jan 17 15:46:17.839167 aaa: Enviando solicitação para o serviço TACACS

2018 Jan 17 15:46:17.840225 aaa: Grupo de métodos configurado com êxito

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

2018 Jan 17 15:46:18.044048 aaa: is_aaa_resp_status_successful é TRUE

2018 Jan 17 15:46:18.044395 aaa: aaa_send_client_response para autenticação. 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 Bem-sucedido

2018 Jan 17 15:46:18.045677 aaa: aaa_cleanup_session

2018 Jan 17 15:46:18.045689 aaa: mts_drop de msg de solicitação

2018 Jan 17 15:46:18.045699 aaa: aaa_req deve ser liberada.

2018 Jan 17 15:46:18.045715 aaa: aaa_process_fd_set

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

2018 Jan 17 15:46:18.045732 aaa: aaa_enable_info_config: GET_REQ para uma mensagem de erro de login

2018 Jan 17 15:46:18.045738 aaa: recuperou o valor de retorno da operação de configuração:item de segurança desconhecido

Informações Relacionadas

O comando Ethanalyzer na cli do FX-OS solicitará uma senha quando a autenticação TACACS/RADIUS estiver habilitada. Esse comportamento é causado por um bug.

ID do bug: CSCvg87518