

Configurar a autenticação TACACS da prima 3.1 contra ISE 2.x

Índice

[Introdução](#)

[Requisitos](#)

[Configurar](#)

[Apronte a configuração](#)

[Configuração ISE](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar a infraestrutura principal para autenticar através do TACACS com ISE 2.x.

Requisitos

Cisco recomenda que você tem um conhecimento básico destes assuntos:

- Identity Services Engine (ISE)
- Infraestrutura principal

Configurar

Sistema de controle de redes 3.1 da prima de Cisco

Motor 2.0 do serviço da identidade de Cisco ou mais atrasado.

(Nota: O ISE apoia somente o TACACS que começa com versão 2.0, contudo é possível configurar a prima para usar o raio. A prima inclui a lista de atributos RADIUS além do que o TACACS se você preferiria usar o raio, com uma versão mais velha do ISE ou de uma solução da terceira parte.)

Configuração principal

Navigate à seguinte tela: A administração/usuários, papéis & AAA dos usuários como visto abaixo.

Uma vez que, seleciona a aba dos server TACACS+, a seguir selecione a opção Server adicionar TACACS+ no canto superior do assistente e seletó vá.

Na tela seguinte a configuração da entrada do servidor de TACACS está disponível (esta terá que

ser feita para cada servidor de TACACS individual)

Administration / Users / Users, Roles & AAA

AAA Mode Settings

Active Sessions

Change Password

Local Password Policy

RADIUS Servers

SSO Server Settings

SSO Servers

TACACS+ Servers

User Groups

Users

Add TACACS+ Server

IP Address

DNS Name

* Port: 49

Shared Secret Format: ASCII

* Shared Secret

* Confirm Shared Secret

* Retransmit Timeout: 5 (secs)

* Retries: 1

Authentication Type: PAP

Local Interface IP: 192.168.10.154

Save Cancel

Aqui você precisará de incorporar o endereço IP de Um ou Mais Servidores Cisco ICM NT ou o endereço DNS do server, assim como a chave secreta compartilhada. Igualmente satisfaça notam o IP da interface local que você gostaria de usar, como este mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT precisa de ser usado mais tarde para o cliente de AAA no ISE.

A fim terminar a configuração na prima. Você precisará de permitir o TACACS sob a administração/usuários/usuários, papéis & AAA sob a aba das configurações de modo AAA.

(Nota: Recomenda-se verificar a reserva da possibilidade à opção local, com SOMENTE em nenhuma resposta de servidor ou sobre em nenhuma opção da resposta ou da falha, especialmente ao testar a configuração)

Administration / Users / Users, Roles & AAA

AAA Mode Settings

AAA Mode

Local RADIUS TACACS+ SSO

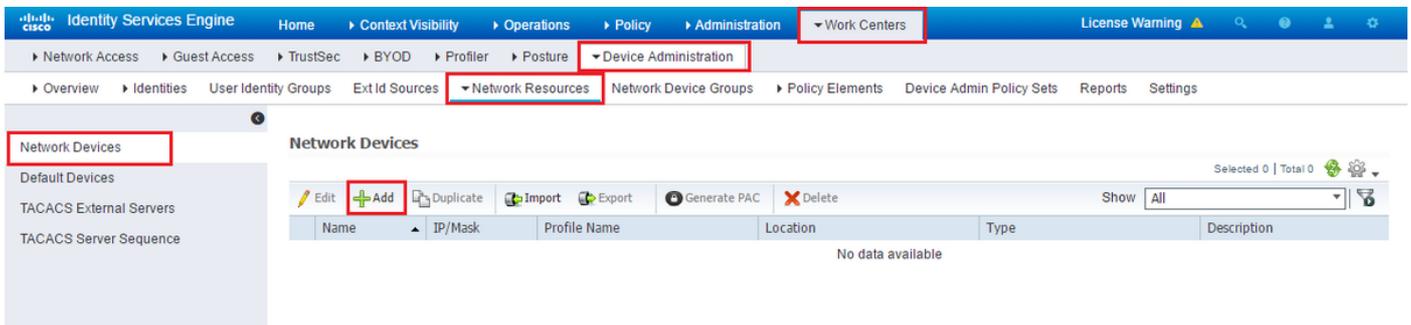
Enable fallback to Local

ONLY on no server respon:

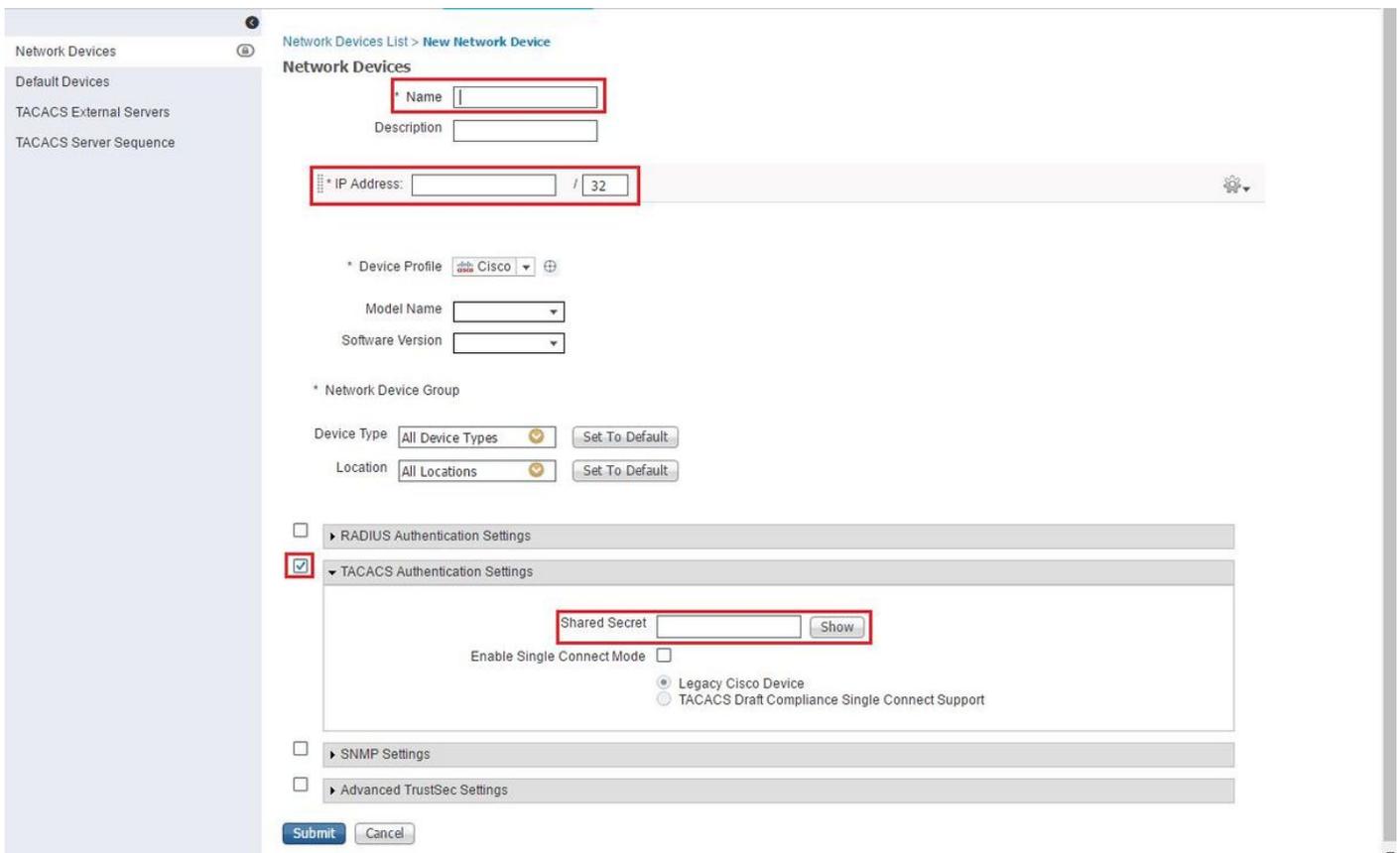
Save

Configuração ISE

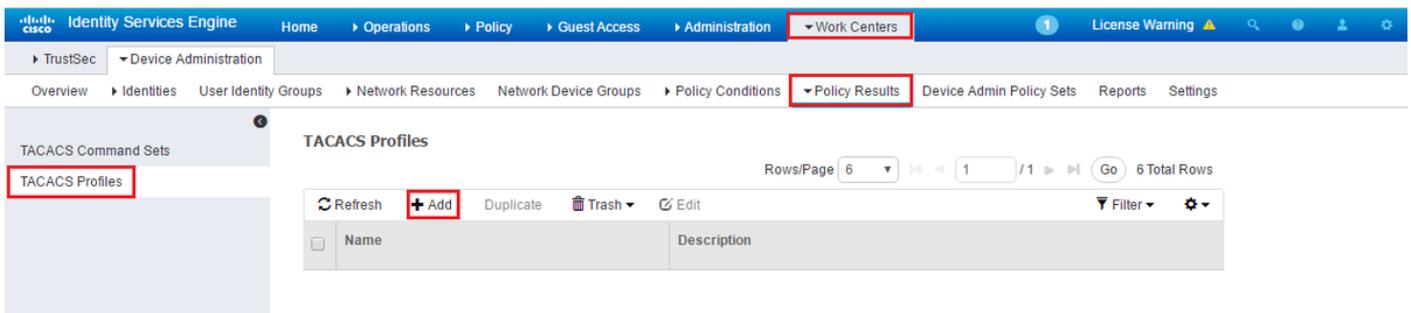
Configurar a prima como um cliente de AAA no ISE em centros de trabalho/em dispositivos do /Network dos recursos do /Network administração do dispositivo/adicionar-la



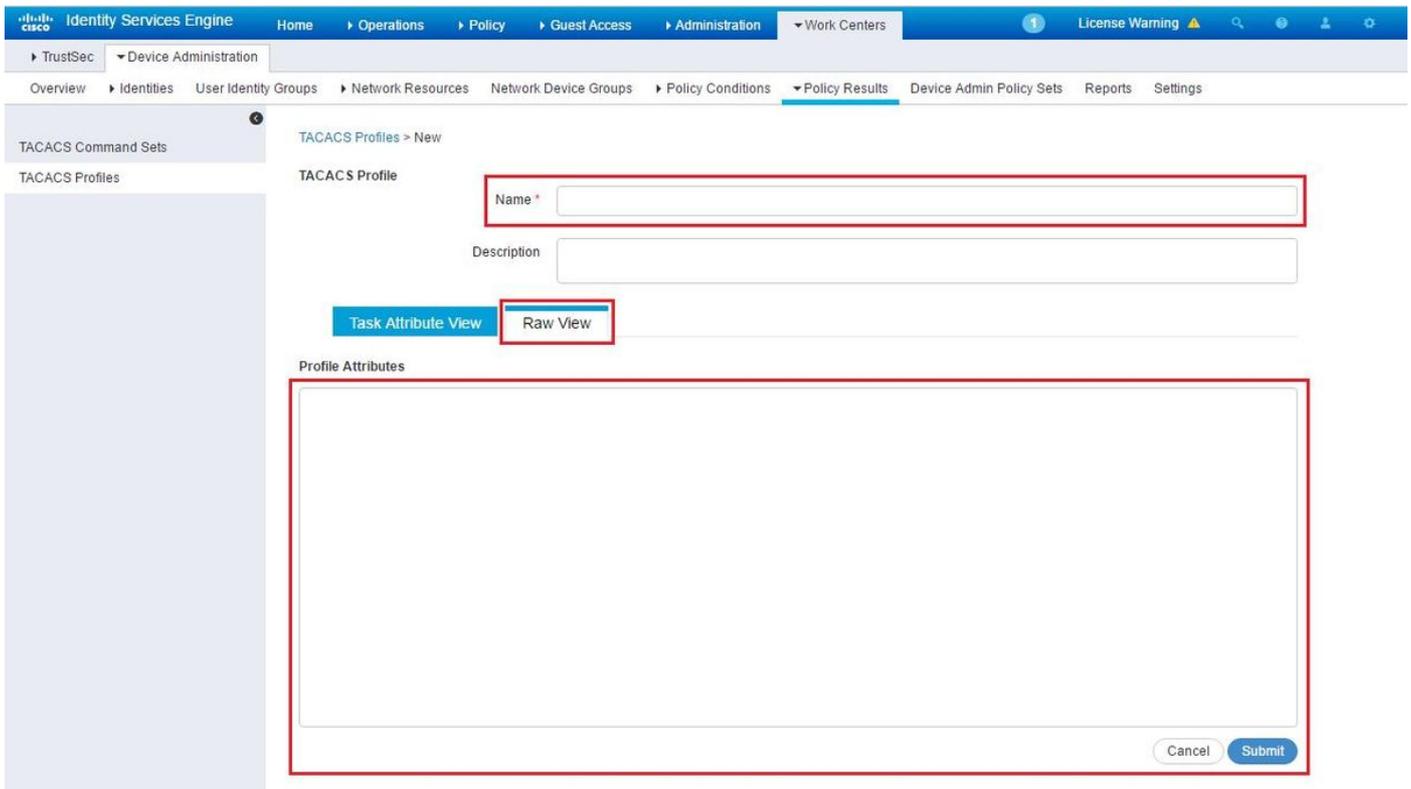
Incorpore a informação para o server principal. Os atributos requerido que você precisa de incluir são nome, endereço IP de Um ou Mais Servidores Cisco ICM NT, selecionam a opção para o TACACS e o segredo compartilhado. Você pode adicionalmente desejar adicionar um tipo de dispositivo, especificamente para a prima, a fim usar-se mais tarde como uma circunstância para a regra da autorização ou a outra informação, porém esta é opcional.



Crie então um resultado do perfil TACACS para enviar os atributos requerido do ISE para aprontar, para fornecer o nível correto do acesso. Navegue aos centros de trabalho/resultados da política/perfis de Tacacs e selecione a opção adicionar.



Configurar o nome, e use a opção crua da vista a fim incorporar os atributos sob a caixa dos atributos do perfil. Os atributos virão do server próprio da primeira demão.



Obtenha os atributos sob a administração/usuários dos usuários, papéis & tela AAA, e selecione a aba dos grupos de usuário. Aqui você seleciona o nível de grupo do acesso que você deseja fornecer. Neste exemplo de admin alcance é fornecido selecionando a lista de tarefas apropriada no lado esquerdo.

Administration / Users / Users, Roles & AAA

AAA Mode Settings	User Groups			
Active Sessions	Group Name	Members	Audit Trail	View Task
Change Password	Admin	JP		Task List
Local Password Policy	Config Managers			Task List
RADIUS Servers	Lobby Ambassador	User1 , CostaRica , Yita		Task List
SSO Server Settings	Monitor Lite			Task List
SSO Servers	NBI Credential			Task List
TACACS+ Servers	NBI Read			Task List
User Groups	NBI Write			Task List
Users	North Bound API			Task List
	Root	root		Task List
	Super Users			Task List
	System Monitoring			Task List
	User Assistant			Task List
	User Defined 1			Task List
	User Defined 2			Task List
	User Defined 3			Task List
	User Defined 4			Task List
	mDNS Policy Admin			Task List

Copie todos os atributos feitos sob encomenda TACACS.

- AAA Mode Settings
- Active Sessions
- Change Password
- Local Password Policy
- RADIUS Servers
- SSO Server Settings
- SSO Servers
- TACACS+ Servers
- User Groups**
- Users

Task List

Please copy and paste the appropriate protocol data below into the custom/vendor-specific attribute field in your AAA server.

TACACS+ Custom Attributes

```
role0=Admin
task0=Discovery Schedule Privilege
task1=Mesh Reports
task2=Saved Reports List
task3=Monitor Menu Access
task4=Device WorkCenter
task5=Inventory Menu Access
task6=Add Device Access
task7=Config Audit Dashboard
task8=Custom NetFlow Reports
task9=Apic Controller Read Access
task10=Configuration Templates Read Access
task11=Alarm Policies Edit Access
task12=High Availability Configuration
task13=View Job
task14=Incidents Alarms Events Access
task15=TAC Case Management Tool
task16=Configure Autonomous Access Point
Templates
task17=Import Policy Update
task18=PnP Profile Read-Write Access
task19=SSO Server AAA Mode
task20=Alarm Resource Access
```

RADIUS Custom Attributes

If the size of the RADIUS attributes on your AAA server is more than 4096 bytes, Please copy ONLY role attributes, application will retrieve the associated TASKS

```
NCS:role0=Admin
NCS:task0=Discovery Schedule Privilege
NCS:task1=Mesh Reports
NCS:task2=Saved Reports List
NCS:task3=Monitor Menu Access
NCS:task4=Device WorkCenter
NCS:task5=Inventory Menu Access
NCS:task6=Add Device Access
NCS:task7=Config Audit Dashboard
NCS:task8=Custom NetFlow Reports
NCS:task9=Apic Controller Read Access
NCS:task10=Configuration Templates Read Access
NCS:task11=Alarm Policies Edit Access
NCS:task12=High Availability Configuration
NCS:task13=View Job
NCS:task14=Incidents Alarms Events Access
NCS:task15=TAC Case Management Tool
NCS:task16=Configure Autonomous Access Point
Templates
NCS:task17=Import Policy Update
NCS:task18=PnP Profile Read-Write Access
NCS:task19=SSO Server AAA Mode
NCS:task20=Alarm Resource Access
```

Virtual Domain custom attributes are mandatory. To add custom attributes related to Virtual Domains, please click here.

Cole-os então na seção crua da vista do perfil no ISE.

The screenshot shows the Cisco ISE configuration page for a TACACS+ Profile named "Prime". The "Raw View" tab is active, displaying a list of task attributes. The attributes are as follows:

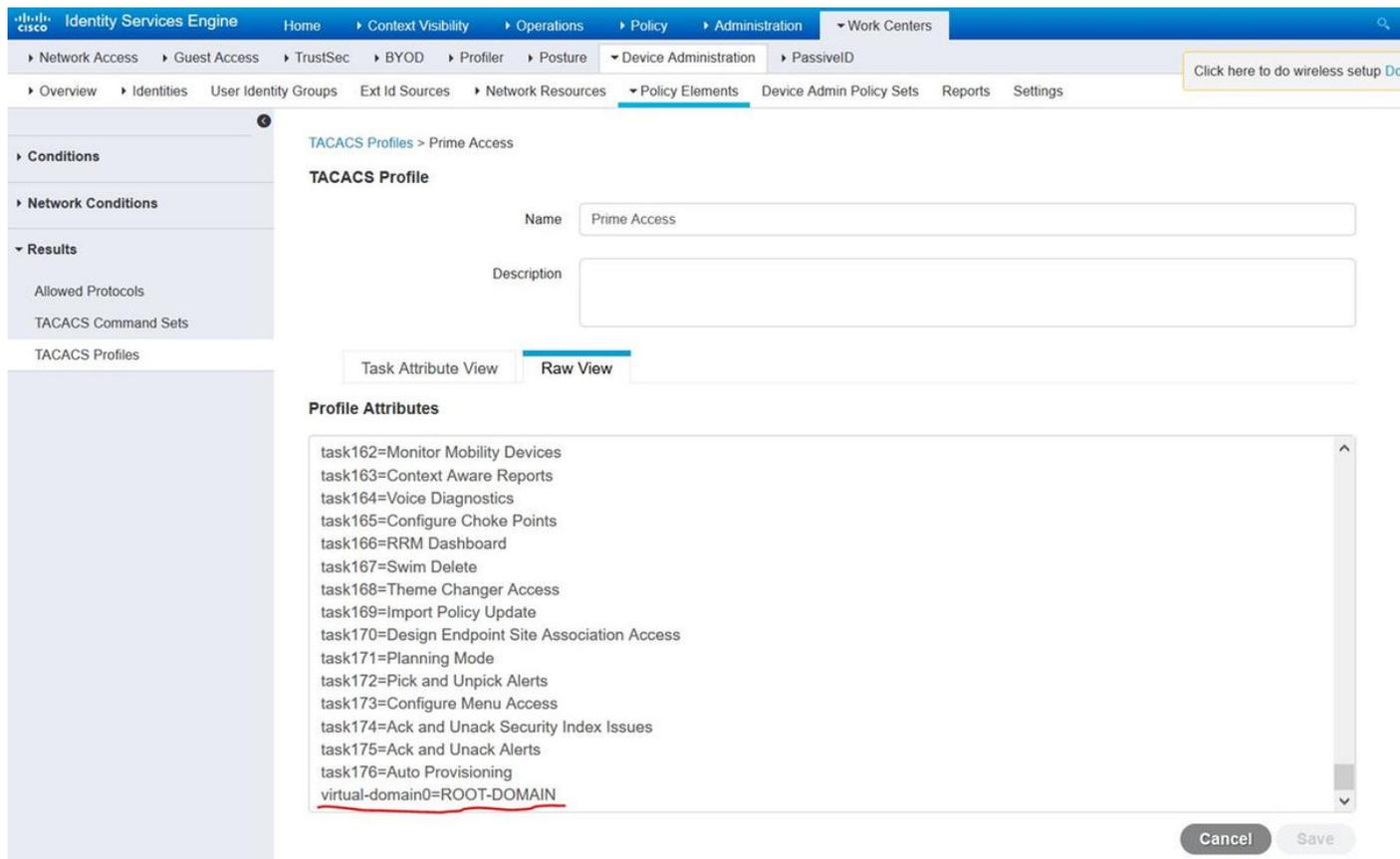
```
role0=Admin
task0=Discovery Schedule Privilege
task1=Mesh Reports
task2=Saved Reports List
task3=Monitor Menu Access
task4=Device WorkCenter
task5=Inventory Menu Access
task6=Add Device Access
task7=Config Audit Dashboard
task8=Custom NetFlow Reports
task9=Apic Controller Read Access
task10=Configuration Templates Read Access
task11=Alarm Policies Edit Access
task12=High Availability Configuration
task13=View Job
```

Os atributos feitos sob encomenda do Domínio Virtual são imperativos. A informação do Raiz-domínio pode ser encontrada sob a administração principal -> Domínios Virtuais.

The screenshot shows the Cisco Prime Infrastructure configuration page for a Virtual Domain named "ROOT-DOMAIN". The configuration fields are as follows:

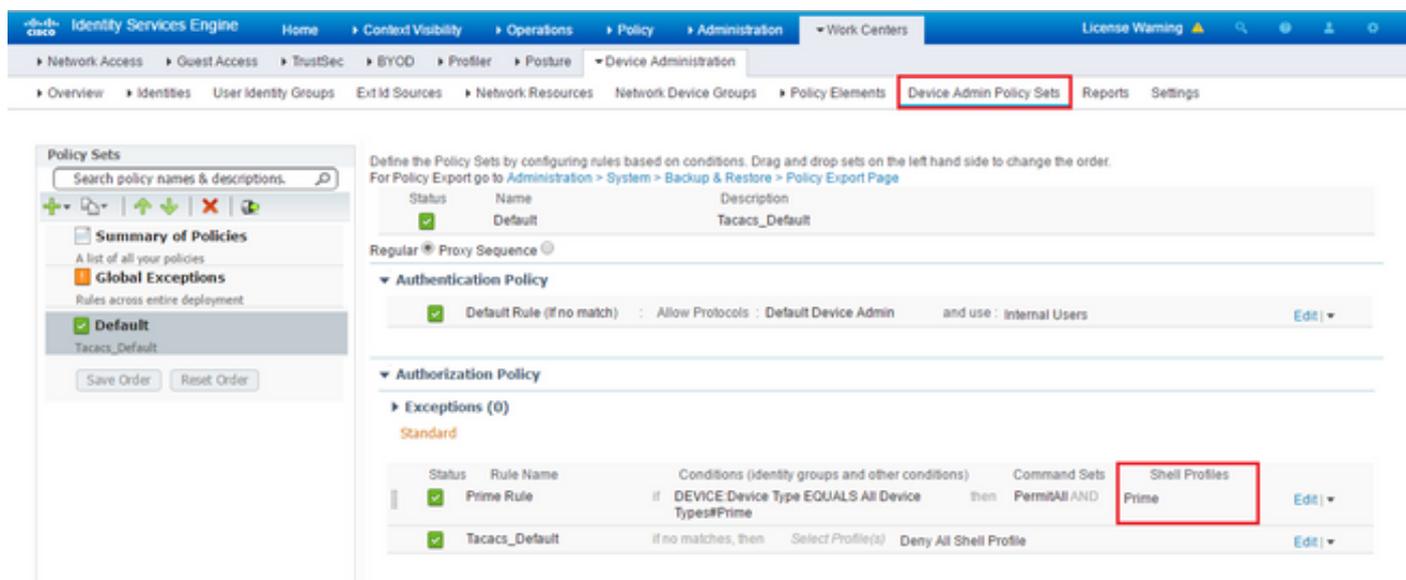
- Name: ROOT-DOMAIN
- Time Zone: -- Select Time Zone --
- Email Address: (empty field)
- Description: ROOT-DOMAIN

O nome do Domínio Virtual principal tem que ser adicionado como o Domain Name do atributo `virtual-domain0="virtual"`



Uma vez que isso é feito tudo você precisa de fazer deve criar uma regra para atribuir o perfil do shell criado na etapa precedente, sob centros de trabalho/política Admin administração do dispositivo/dispositivo ajusta-se

(Nota: As “circunstâncias” variarão segundo o desenvolvimento, porém você pode usar o “tipo de dispositivo” especificamente para a prima ou um outro tipo de filtro tal como o endereço IP de Um ou Mais Servidores Cisco ICM NT da prima, como um do “condicionam” de modo que esta regra filtre corretamente pedidos)



Neste momento a configuração deve estar completa.

Troubleshooting

Se esta configuração é mal sucedida e se o local recua opção era permite na prima, você pode forçar uma falha sobre do ISE, removendo o endereço IP de Um ou Mais Servidores Cisco ICM NT da prima. Isto fará com que o ISE não responda e force o uso de credenciais locais. Se a reserva local é configurada para ser executada em uma rejeição, as contas local ainda trabalharão e fornecerão o acesso ao cliente.

Se o ISE mostra uma autenticação bem sucedida e está combinando a regra correta contudo a prima ainda está rejeitando o pedido que você pode desejar verificar novamente os atributos é configurado corretamente no perfil e nenhum atributo adicional está sendo enviado.