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

Índice

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.)

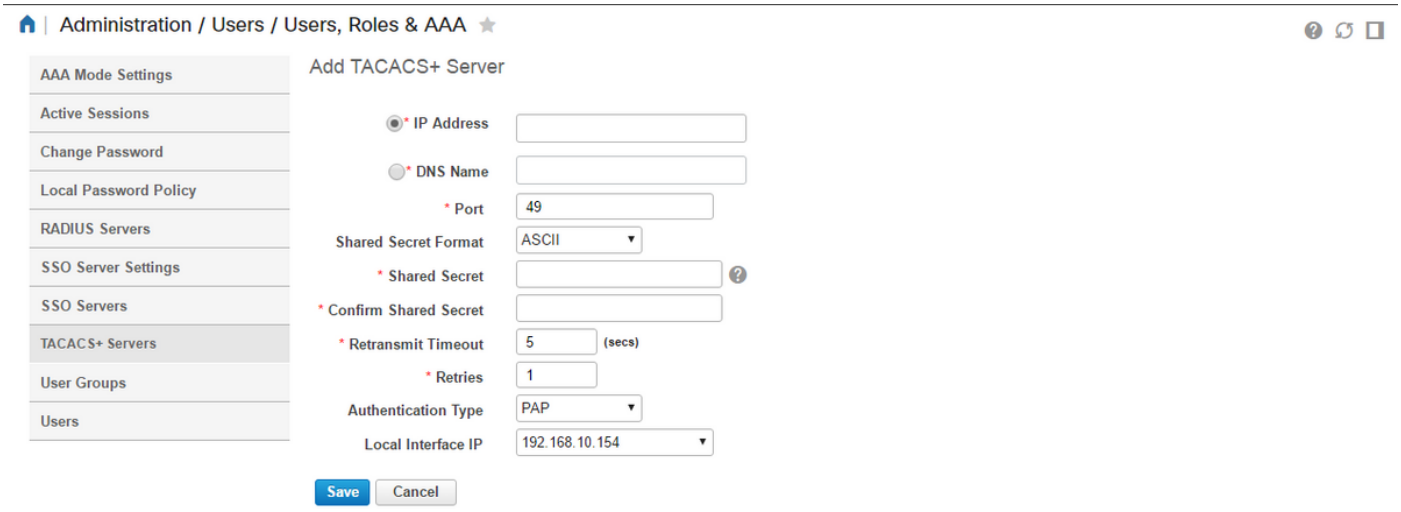
Configuração principal

Navigiate 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 seleto 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)



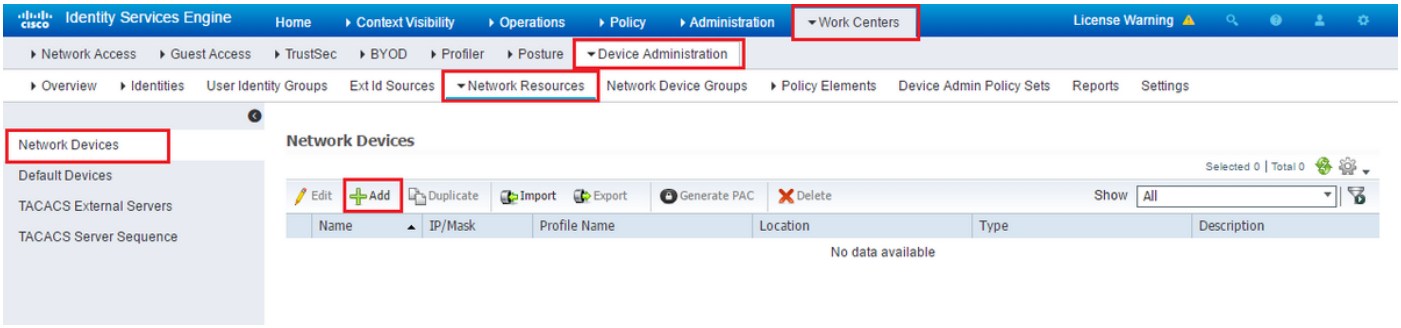
Aqui você precisará de incorporar o endereço IP de Um ou Mais Servidores Cisco ICM NT ou o endereço DNS do server, assim como a chave secreta compartilhada. Igualmente satisfaça notam o IP da interface local que você gostaria de usar, como este mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT 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.

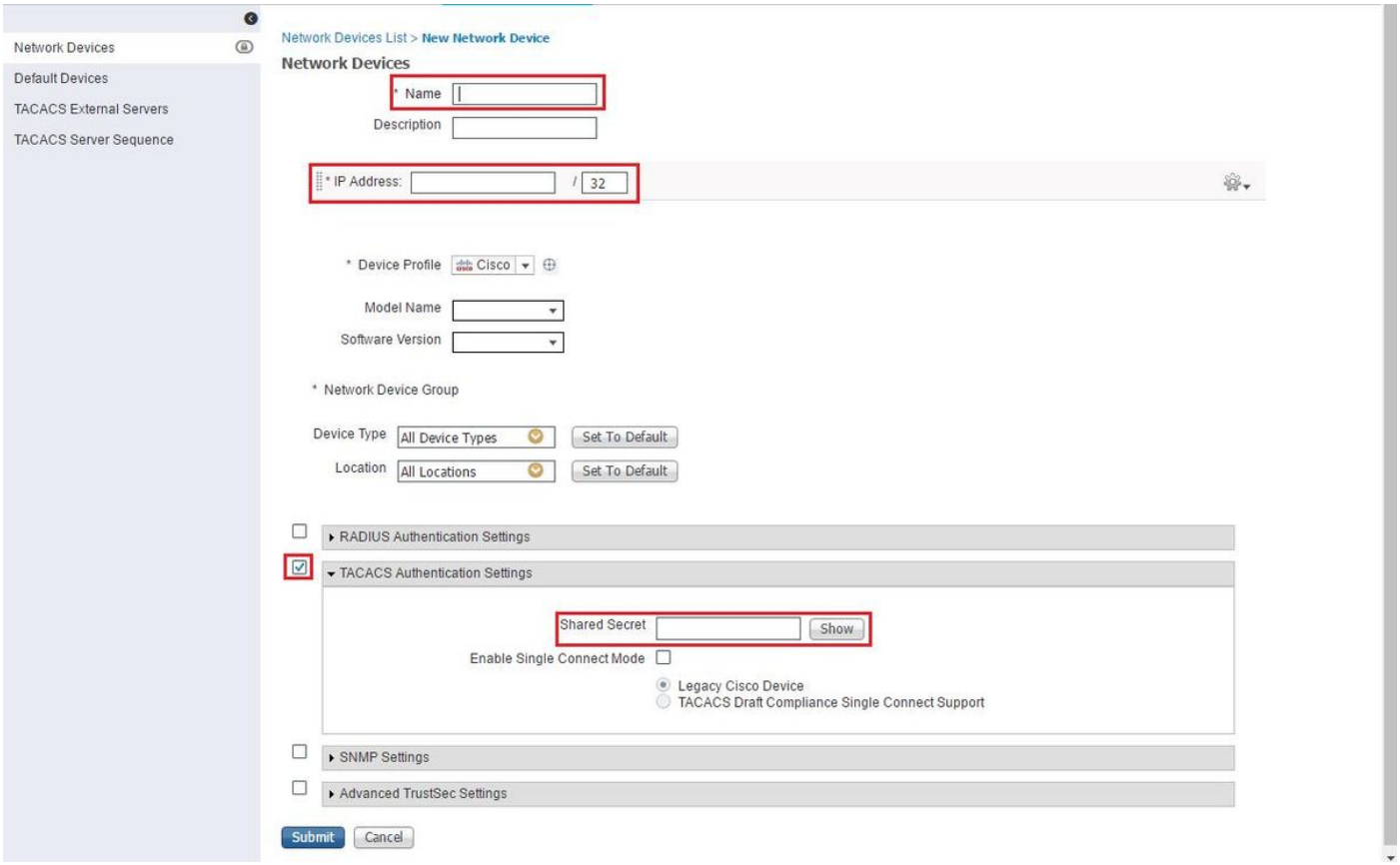
(Nota: Recomenda-se verificar a reserva da possibilidade à opção local, com SOMENTE em nenhuma resposta de servidor ou sobre em nenhuma opção da resposta ou da falha, especialmente ao testar a configuração)

Configuração ISE

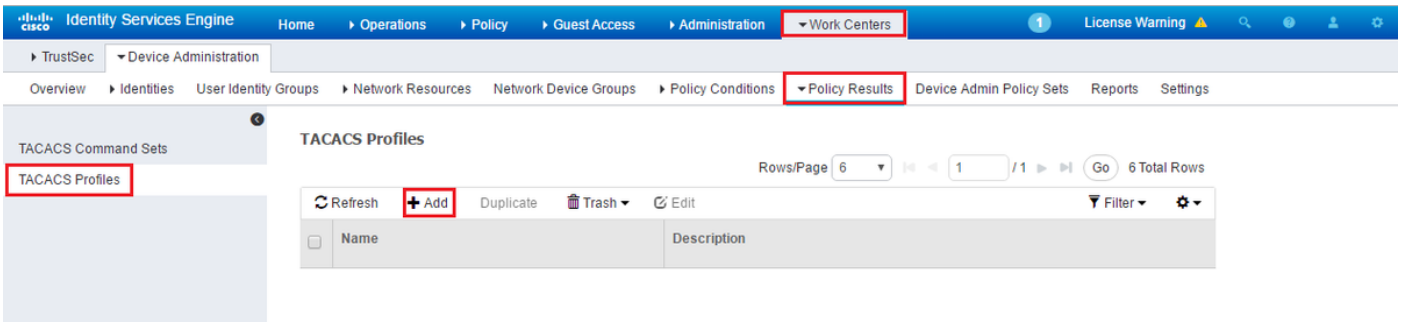
Configurar a prima como um cliente de AAA no ISE em centros de trabalho/em dispositivos do /Network dos recursos do /Network administração do dispositivo/adicionar-la



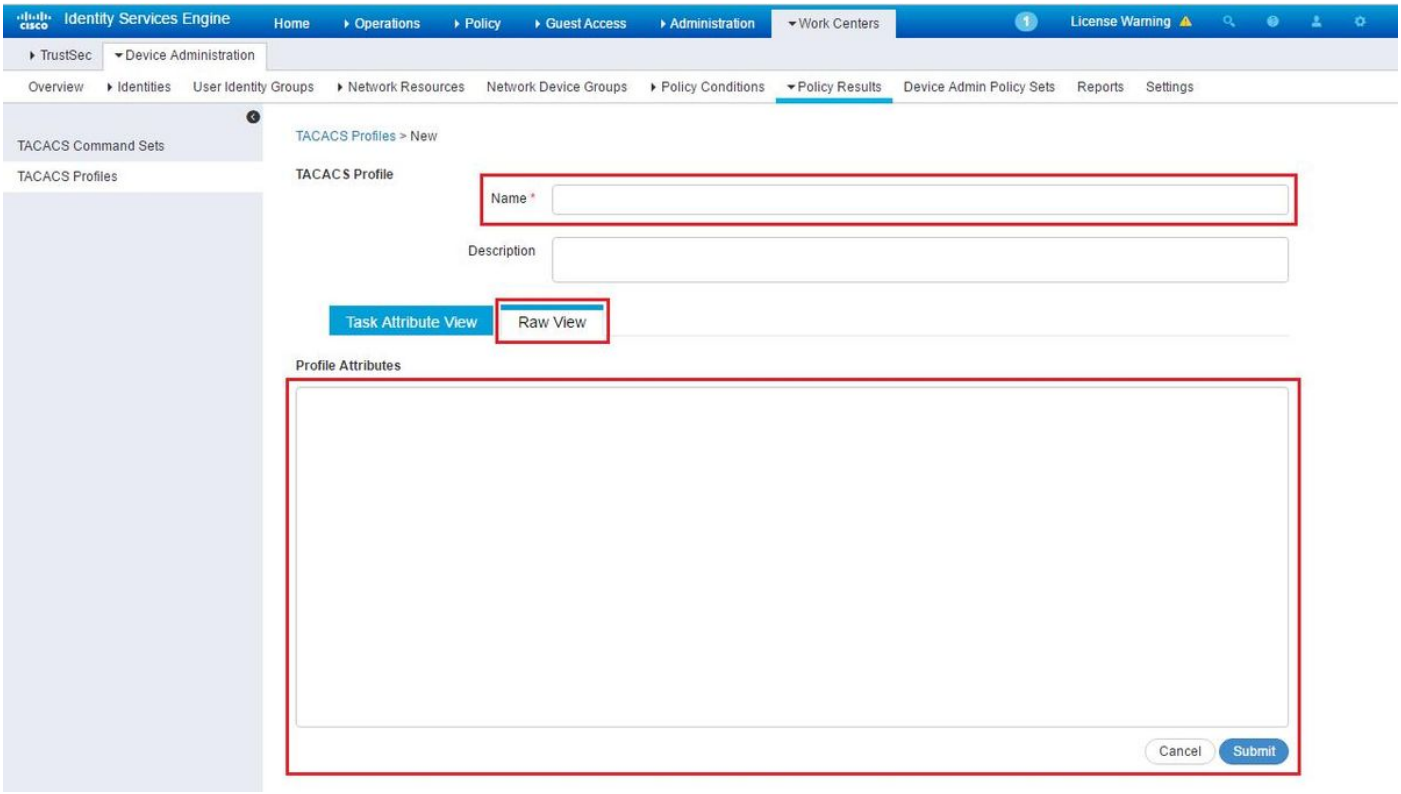
Incorpore a informação para o server principal. Os atributos requerido que você precisa de incluir são nome, endereço IP de Um ou Mais Servidores Cisco ICM NT, selecionam a opção para o TACACS e o segredo compartilhado. Você pode adicionalmente desejar adicionar um tipo de dispositivo, especificamente 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.



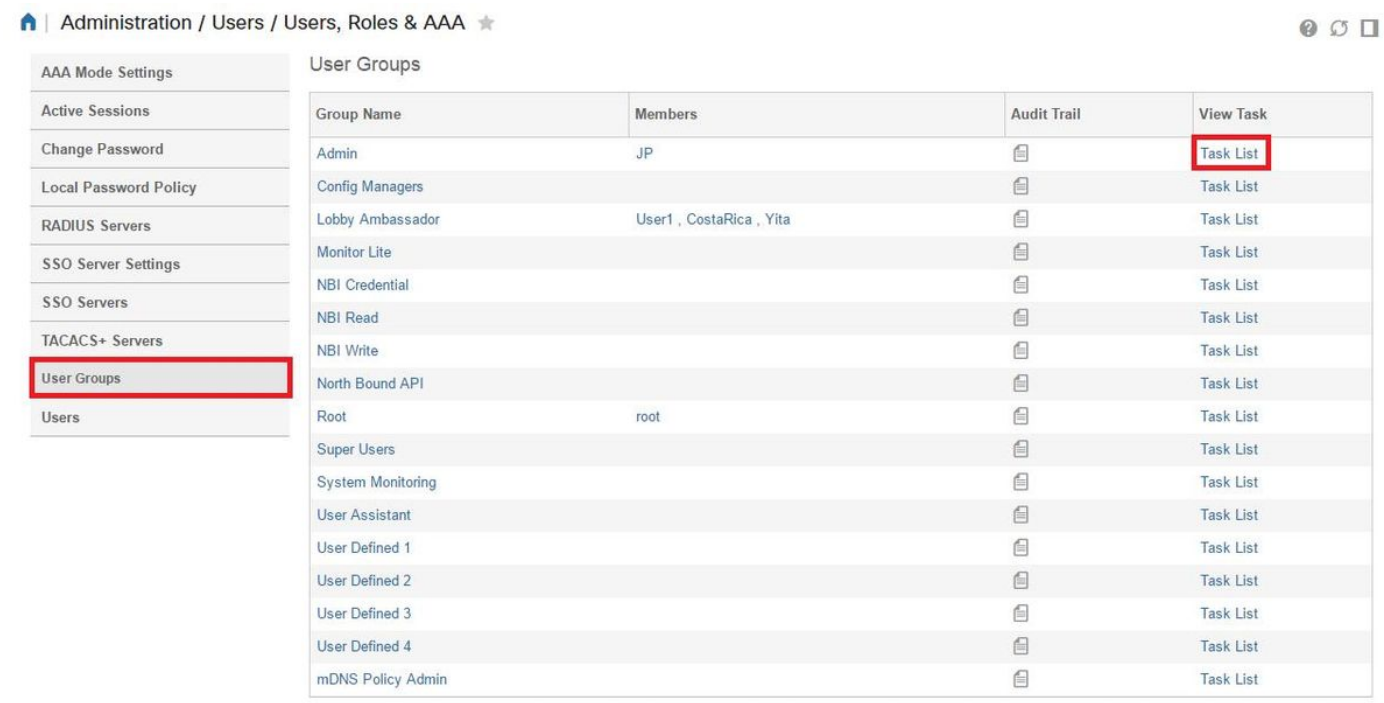
Crie então um resultado do perfil TACACS para enviar os atributos requerido do ISE para aprontar, para fornecer o nível correto do acesso. Navegue aos centros de trabalho/resultados da política/perfis de Tacacs e selecione a opção adicionar.



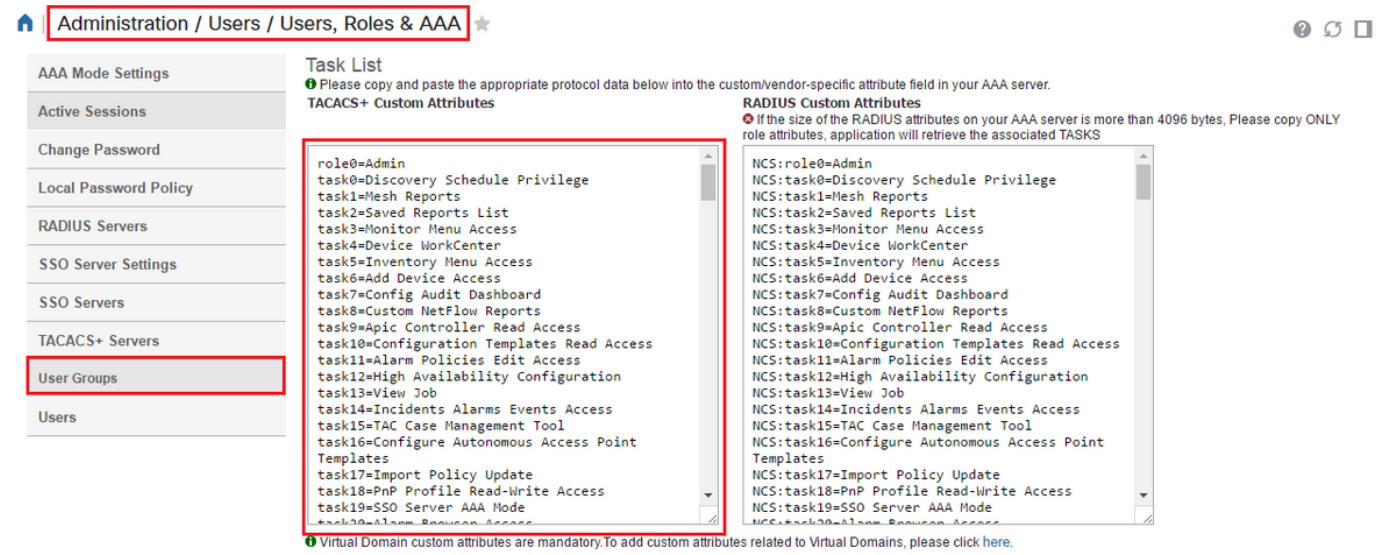
Configurar o nome, e use a opção crua da vista a fim incorporar os atributos sob a caixa dos atributos do perfil. Os atributos virão do server próprio da primeira demão.



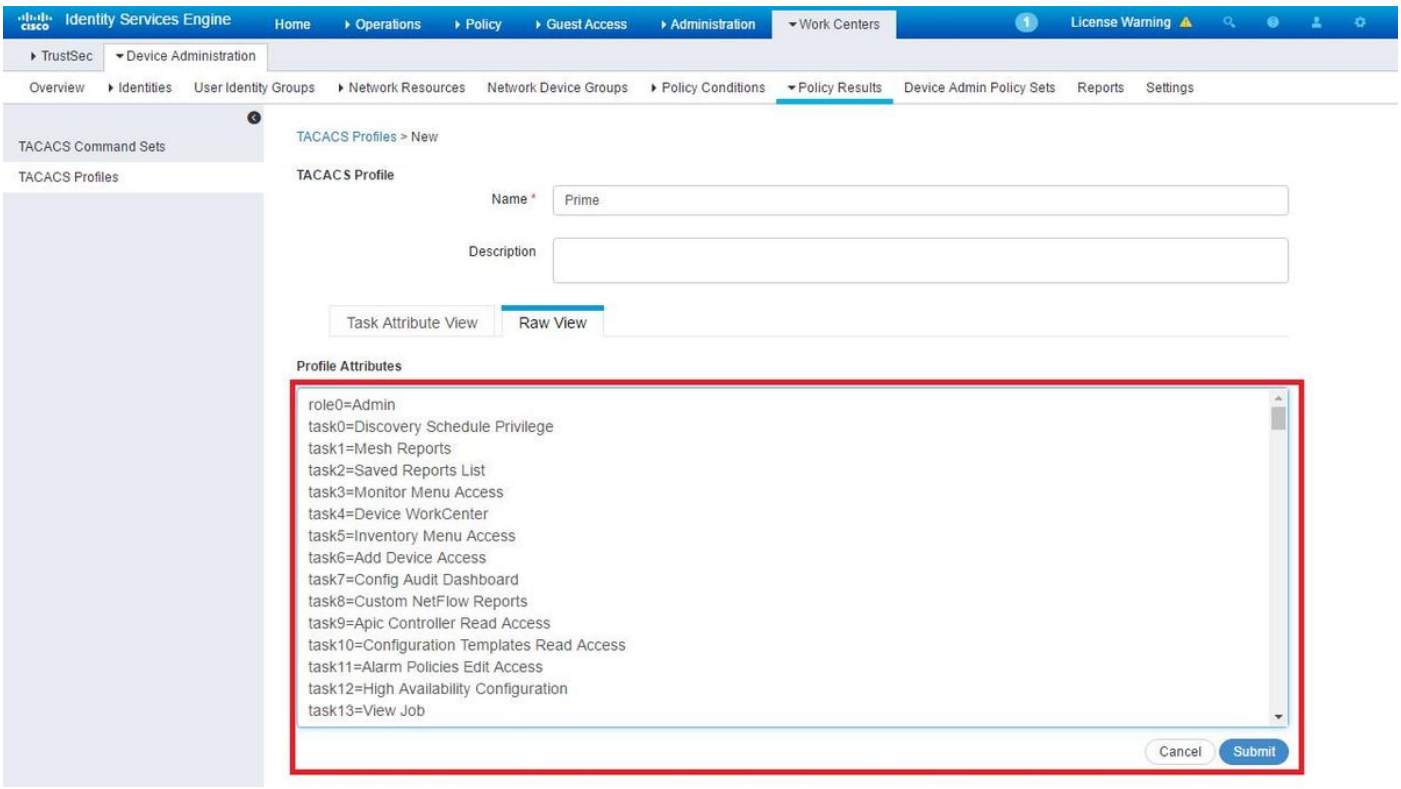
Obtenha os atributos sob a administração/usuários dos usuários, papéis & tela AAA, e selecione a aba dos grupos de usuário. Aqui você seleciona o nível de grupo do acesso que você deseja fornecer. Neste exemplo de admin alcance é fornecido selecionando a lista de tarefas apropriada no lado esquerdo.



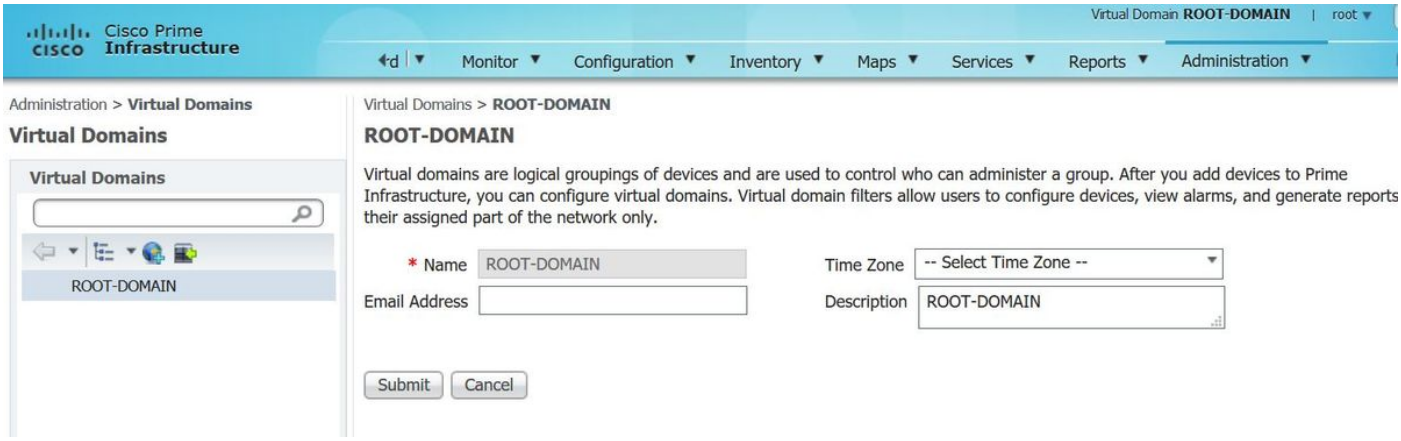
Copie todos os atributos feitos sob encomenda TACACS.



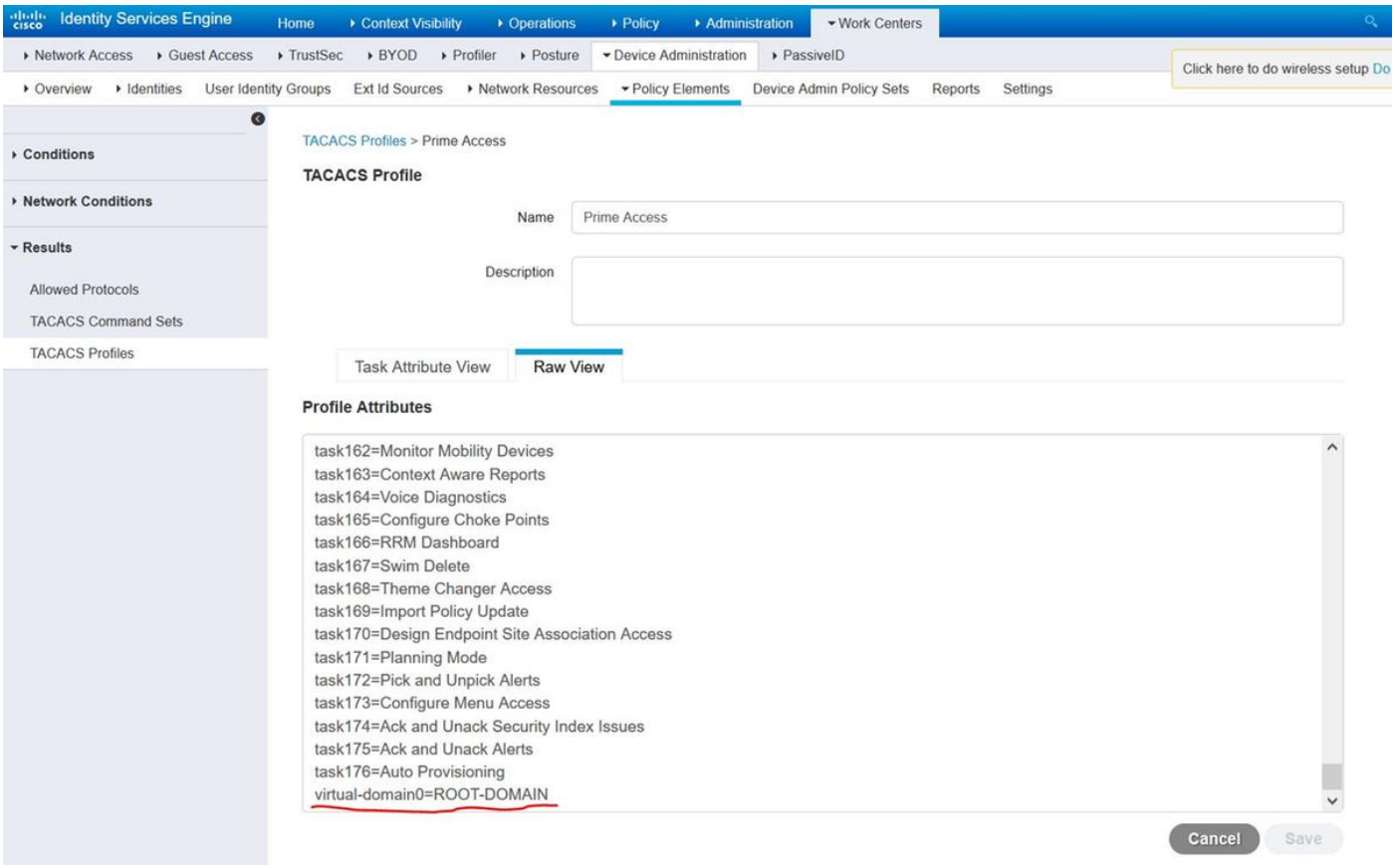
Cole-os então na seção crua da vista do perfil no ISE.



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

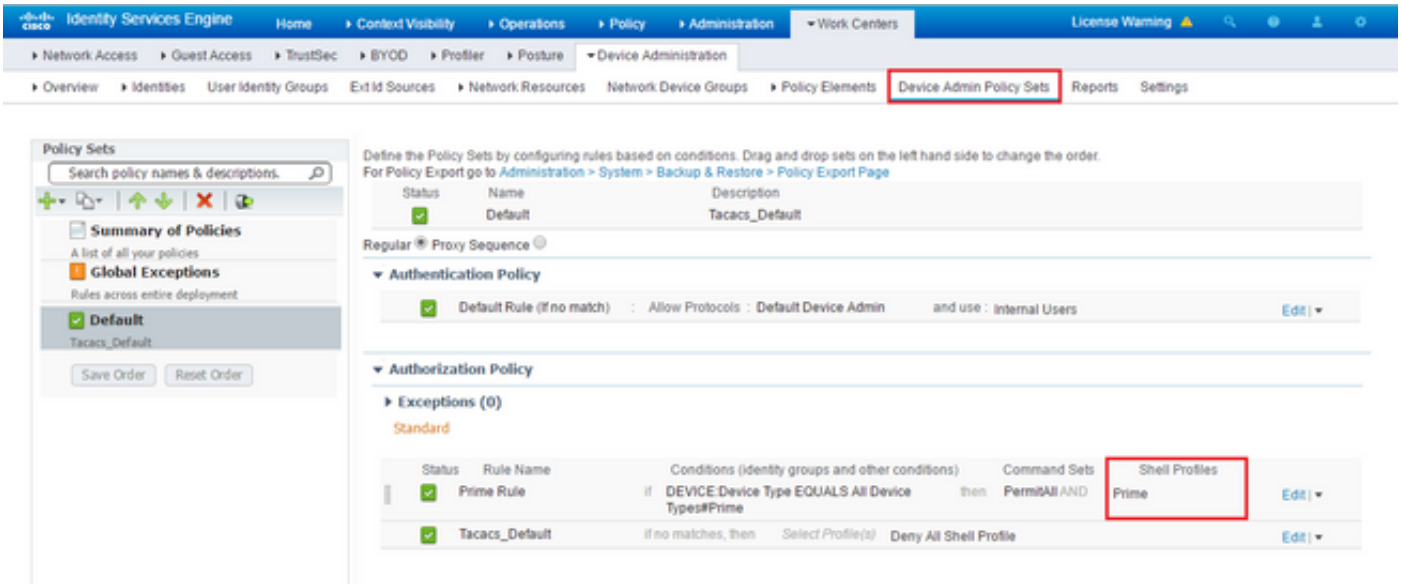


O nome do Domínio Virtual principal tem que ser adicionado como o Domain Name do atributo **virtual-domain0="virtual**"



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.