Autenticación de TACACS de la prima 3.1 de la configuración contra ISE 2.x

Contenido

Introducción

Este documento describe cómo configurar la infraestructura primera para autenticar vía el TACACS con ISE 2.x.

Requisitos

Cisco recomienda que usted tiene un conocimiento básico de estos temas:

- Identity Services Engine (ISE)
- Infraestructura primera

Configurar

Sistema de control de redes 3.1 de la prima de Cisco

Motor 2.0 del servicio de la identidad de Cisco o más adelante.

(Nota: El ISE soporta solamente el TACACS que comienza con la versión 2.0, sin embargo es posible configurar la prima para utilizar el radio. La prima incluye la lista de atributos de RADIUS además del TACACS si usted preferiría utilizar el radio, con una versión anterior del ISE o de una solución del otro vendedor.)

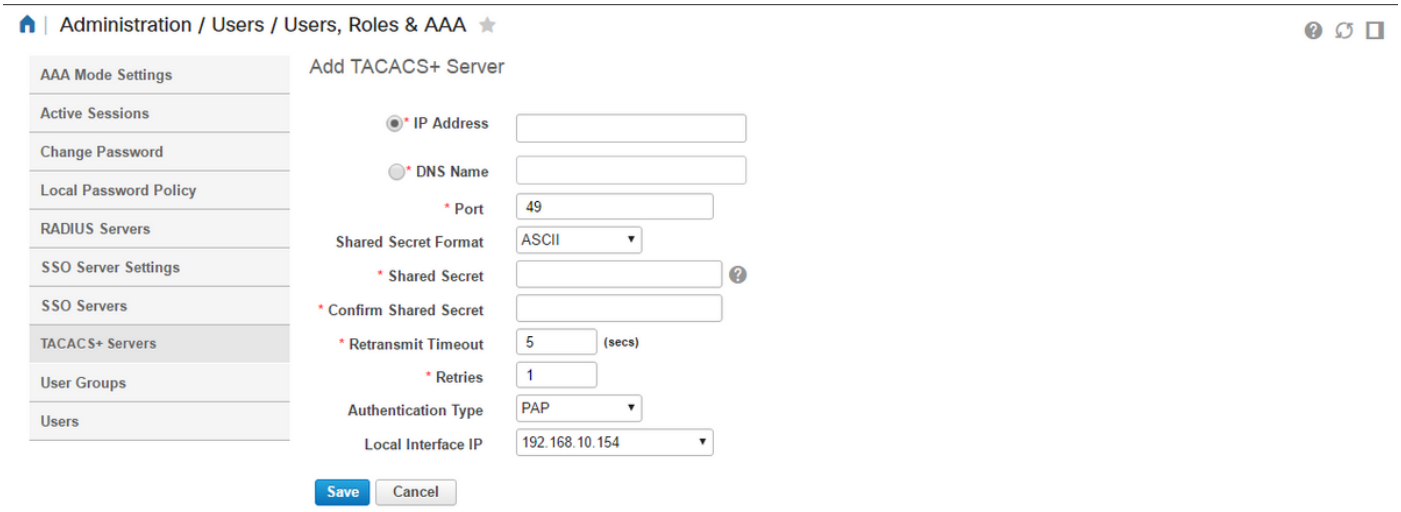
Configuración primera

Navigiate a la pantalla siguiente: La administración/usuarios, papeles y AAA de los usuarios según lo visto abajo.

Una vez que, selecciona el lengueta de los servidores TACACS+, después seleccione la opción del servidor del agregar TACACS+ en la esquina derecha superior y selecto vaya.

En la siguiente pantalla la configuración de la entrada del servidor TACACS está disponible (ésta

tendrá que ser hecha para cada servidor TACACS individual)



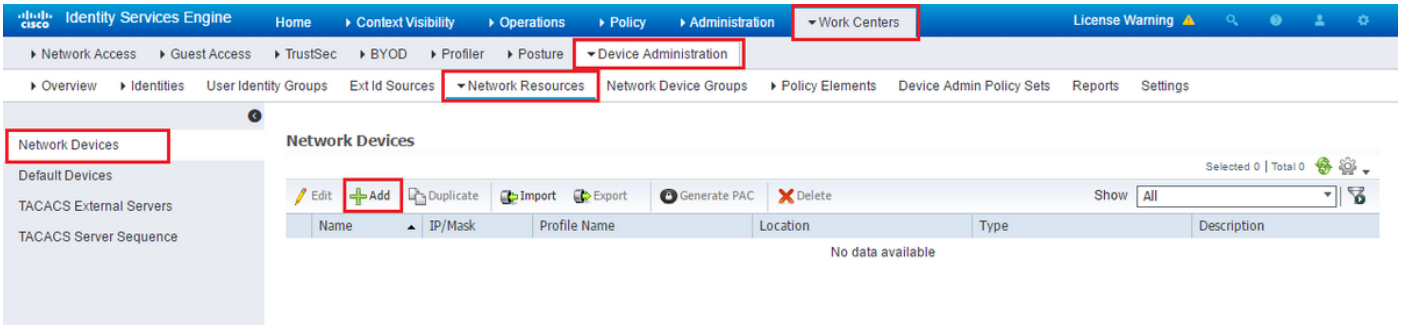
Aquí usted necesitará ingresar el IP Address o la dirección de DNS del servidor, así como la clave secreta compartida. También satisfaga observan el IP de la interfaz local que usted quisiera utilizar, como esta misma dirección IP necesita ser utilizada para el cliente AAA en el ISE después.

Para completar la configuración en la prima. Usted necesitará habilitar el TACACS bajo la administración/los usuarios/los usuarios, los papeles y el AAA bajo lengueta de las configuraciones de modo AAA.

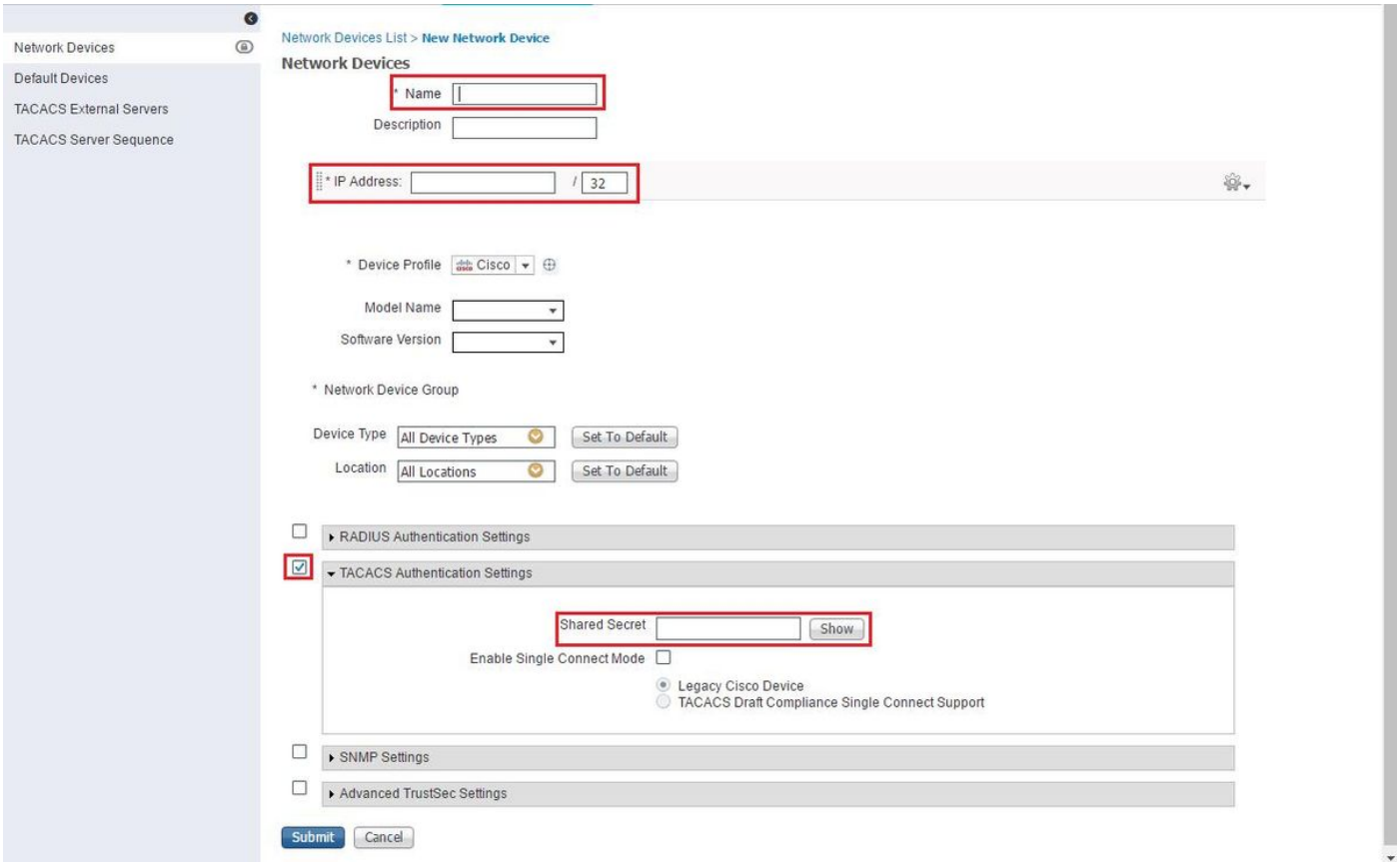
(Nota: Se recomienda para marcar el retraso del permiso a la opción local, con SOLAMENTE en ninguna respuesta del servidor o encendido la ninguna opción de la respuesta o del error, especialmente mientras que prueba la configuración)

Configuración ISE

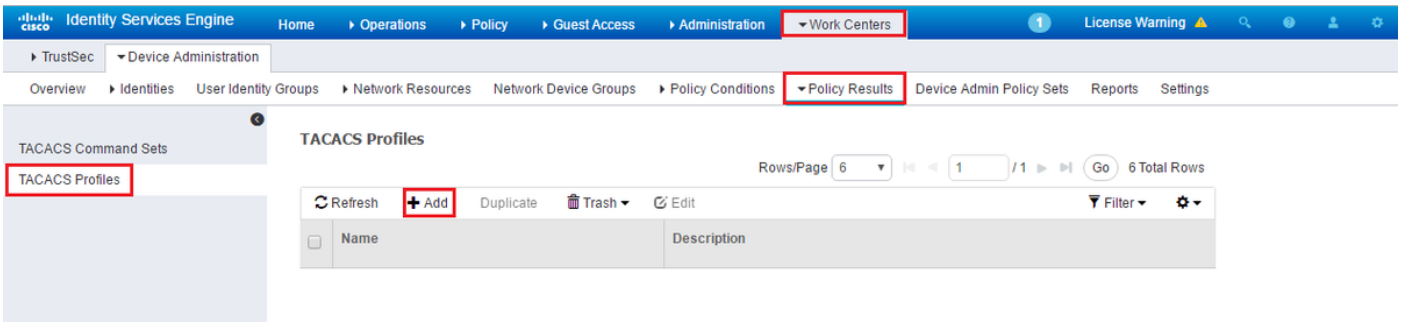
Configure la prima como cliente AAA en el ISE en los centros de trabajo/Device Administration (Administración del dispositivo) los dispositivos del /Network de los recursos del /Network/agregue



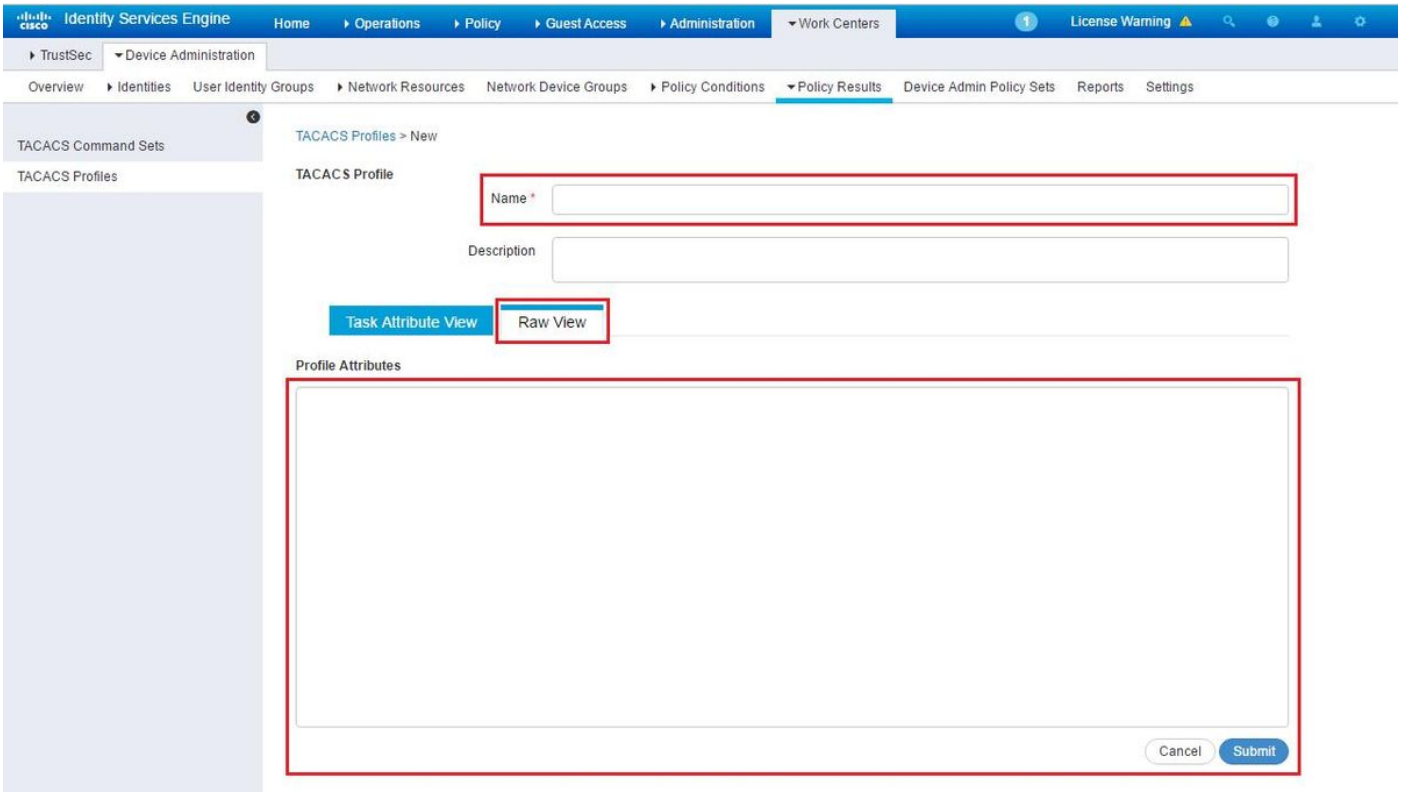
Ingrese la información para el servidor primero. Los atributos requeridos que usted necesita incluir son nombre, dirección IP, seleccionan la opción para el TACACS y el secreto compartido. Usted puede desear además agregar un tipo de dispositivo, específicamente para la prima, para utilizar después como condición para la regla de la autorización o la otra información, no obstante ésta es opcional.



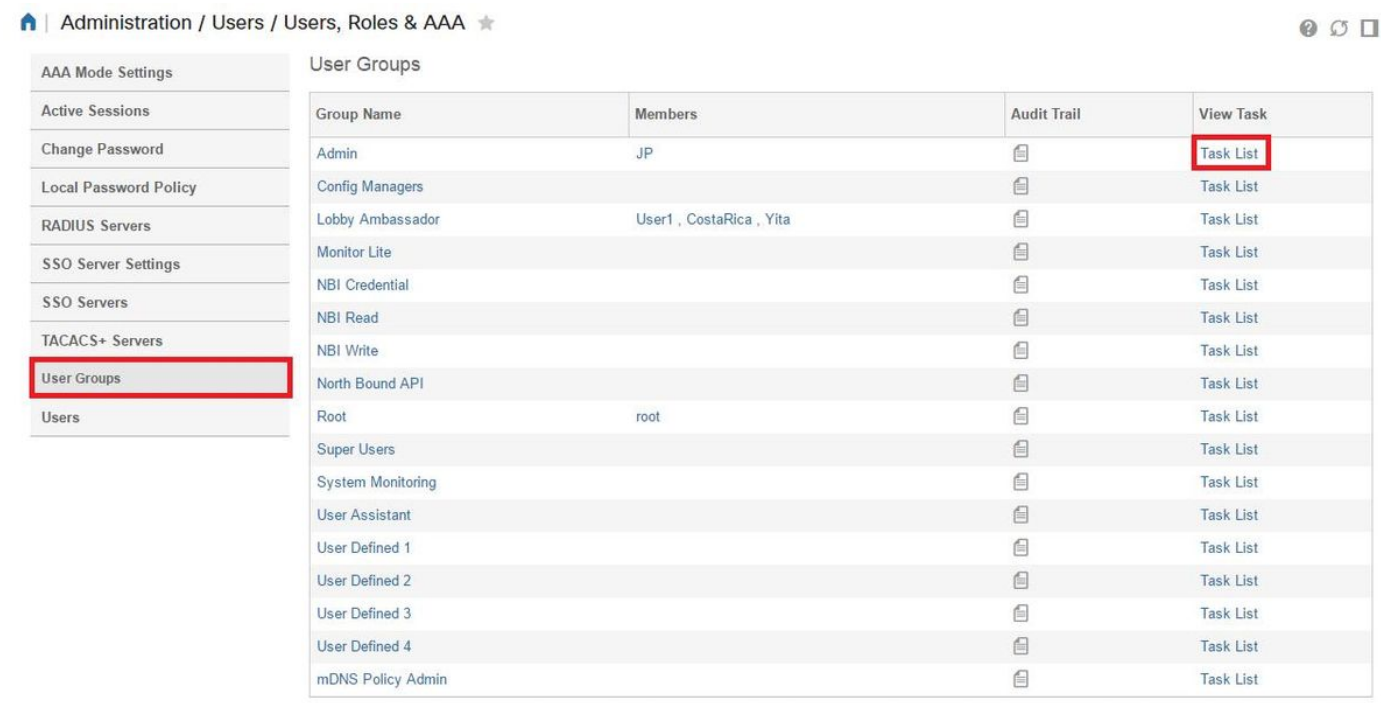
Entonces cree un resultado del perfil TACACS para enviar los atributos requeridos del ISE para preparar, proporcionar el nivel correcto de acceso. Navegue a los centros de trabajo/a los resultados de la directiva/a los perfiles de Tacacs y seleccione la opción del agregar.



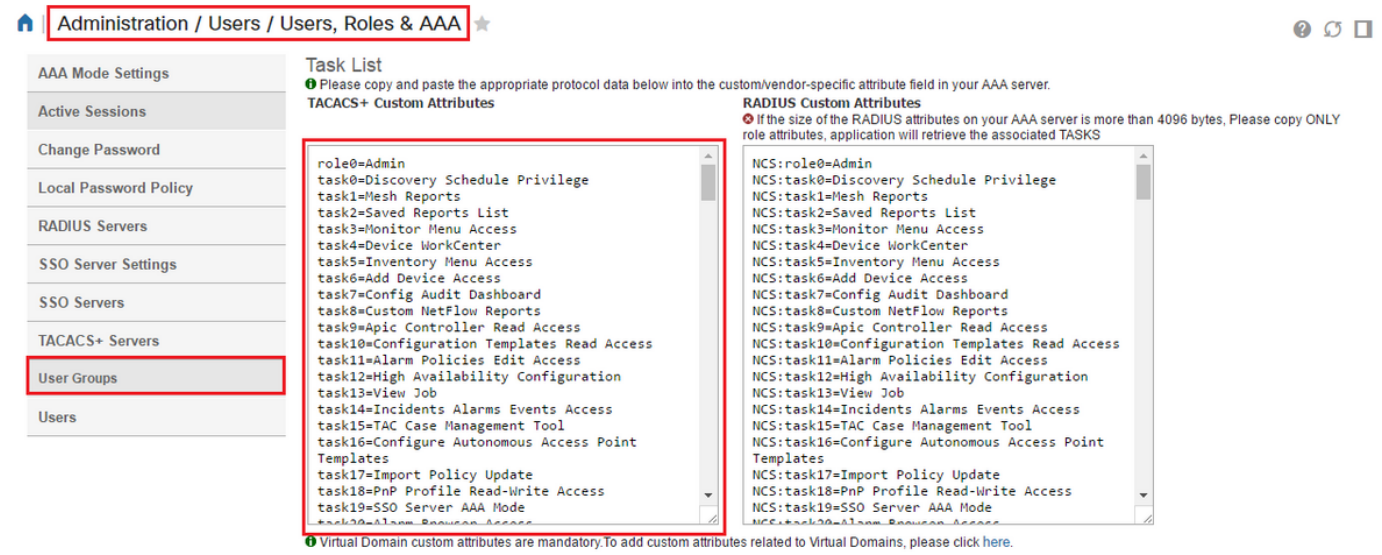
Configure el nombre, y utilice la opción sin procesar de la visión para ingresar los atributos bajo el rectángulo de los atributos del perfil. Los atributos vendrán del servidor sí mismo de la cartilla.



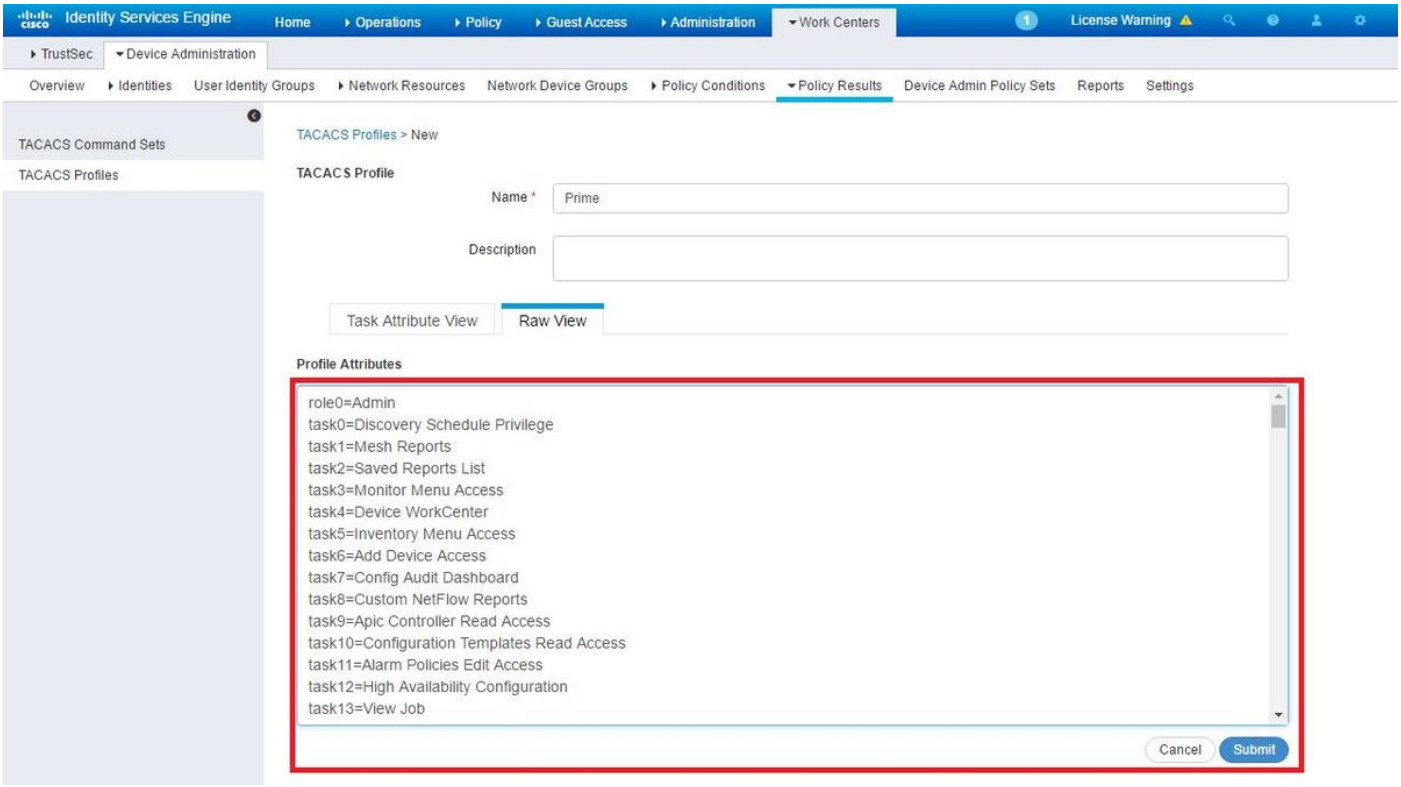
Consiga los atributos bajo la administración/los usuarios de los usuarios, los papeles y la pantalla AAA, y seleccione la lengueta de los grupos de usuarios. Aquí usted selecciona el nivel de grupo de acceso que usted desea proporcionar. En este admin de ejemplo el acceso es proporcionado seleccionando la lista de tareas apropiada en el lado izquierdo.



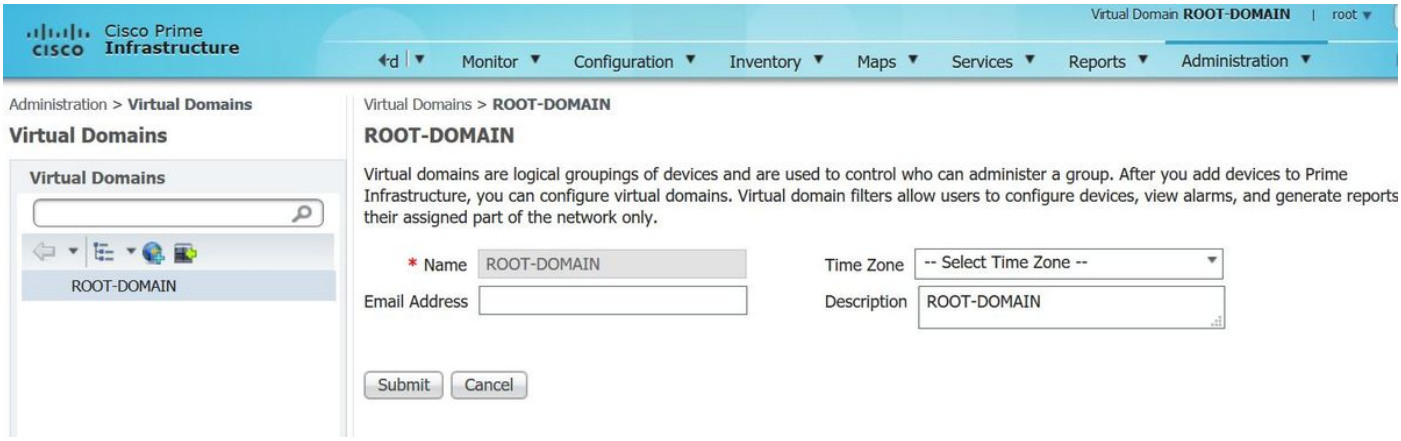
Copie todos los atributos personalizados TACACS.



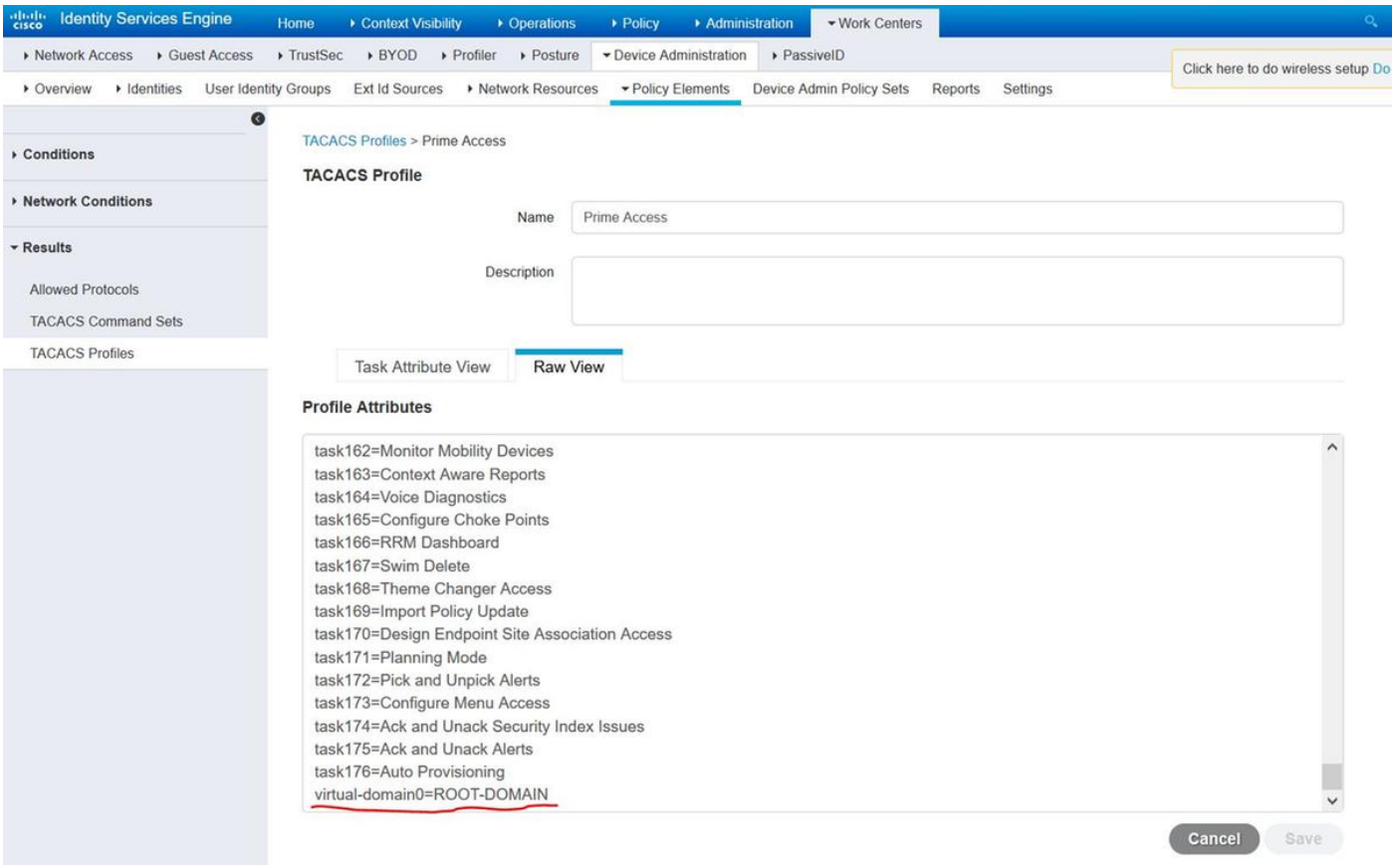
Entonces pegúelos en la sección sin procesar de la visión del perfil en el ISE.



Los atributos personalizados del dominio virtual son obligatorios. La información del Raíz-dominio se puede encontrar bajo administración primera - > los dominios virtuales.

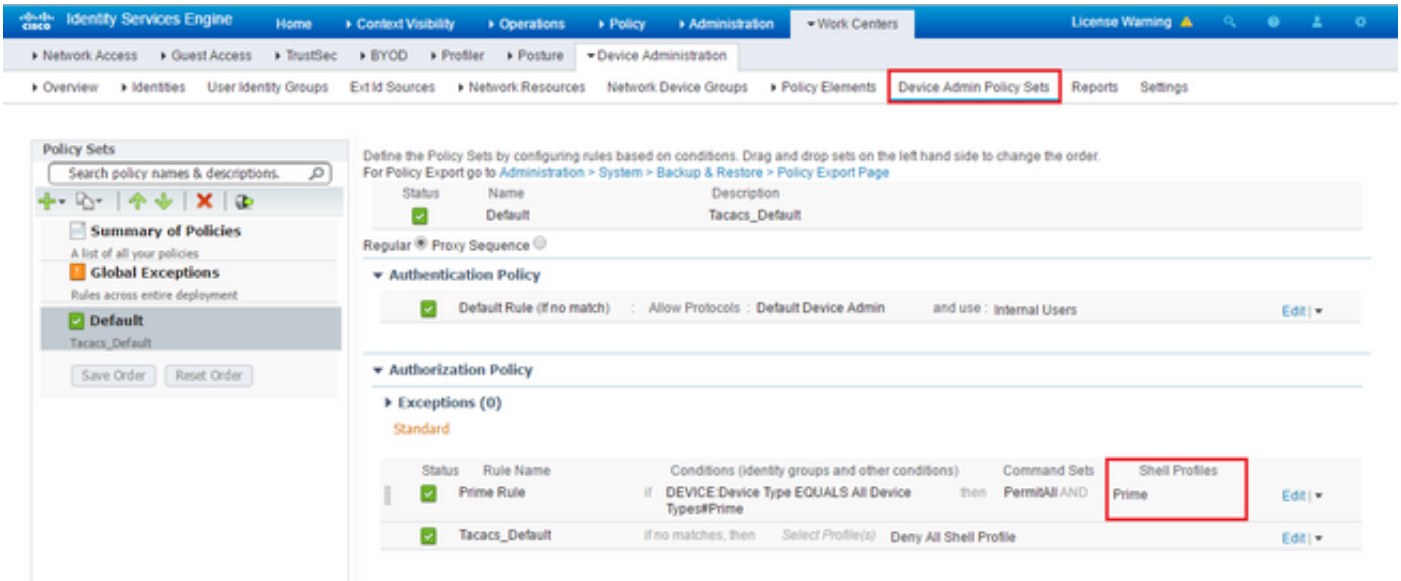


El nombre del dominio virtual primero tiene que ser agregado como Domain Name del atributo **virtual-domain0="virtual**"



Una vez que eso se hace todos usted necesita hacer debe crear una regla para asignar el perfil del shell creado en el paso anterior, bajo los centros de trabajo/Device Administration (Administración del dispositivo)/directiva Admin del dispositivo fija

(Nota: Las “condiciones” variarán dependiendo del despliegue, no obstante usted puede utilizar el “tipo de dispositivo” específicamente para la prima u otro tipo de filtro tal como dirección IP de la prima, como una de “condicionan” de modo que esta regla filtre correctamente las peticiones)



En este momento la configuración debe ser completa.

Troubleshooting

Si esta configuración es fracasada y si bajan el locales opción eran permiso en la prima, usted puede forzar un fall encima del ISE, quitando la dirección IP de la prima. Esto hará el ISE no responder y forzar el uso de las credenciales locales. Si el retraso local se configura para ser realizado en un rechazo, las cuentas locales todavía trabajarán y proporcionarán el acceso al cliente.

Si el ISE muestra una autenticación satisfactoria y está correspondiendo con la regla correcta sin embargo la prima todavía está rechazando la petición que usted puede desear para comprobar los atributos con minuciosidad se configura correctamente en el perfil y no se está enviando ningunos atributos adicionales.