Integración del sistema FireSIGHT con ACS 5.x para la autenticación de usuarios RADIUS

Contenido

Introducción

Este documento describe los pasos de configuración requeridos para integrar un Cisco FireSIGHT Management Center (FMC) o un dispositivo administrado con Firepower con Cisco Secure Access Control System 5.x (ACS) para la autenticación de usuario del servicio de usuario de acceso telefónico de autenticación remota (RADIUS).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración inicial del sistema FireSIGHT y los dispositivos administrados a través de la GUI o el shell
- Configuración de las políticas de autenticación y autorización en ACS 5.x
- Conocimiento básico de RADIUS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure Access Control System 5.7 (ACS 5.7)
- Cisco FireSight Manager 5.4.1

Las versiones anteriores son las últimas versiones disponibles actualmente. La función es compatible con todas las versiones de ACS 5.x y FMC 5.x.

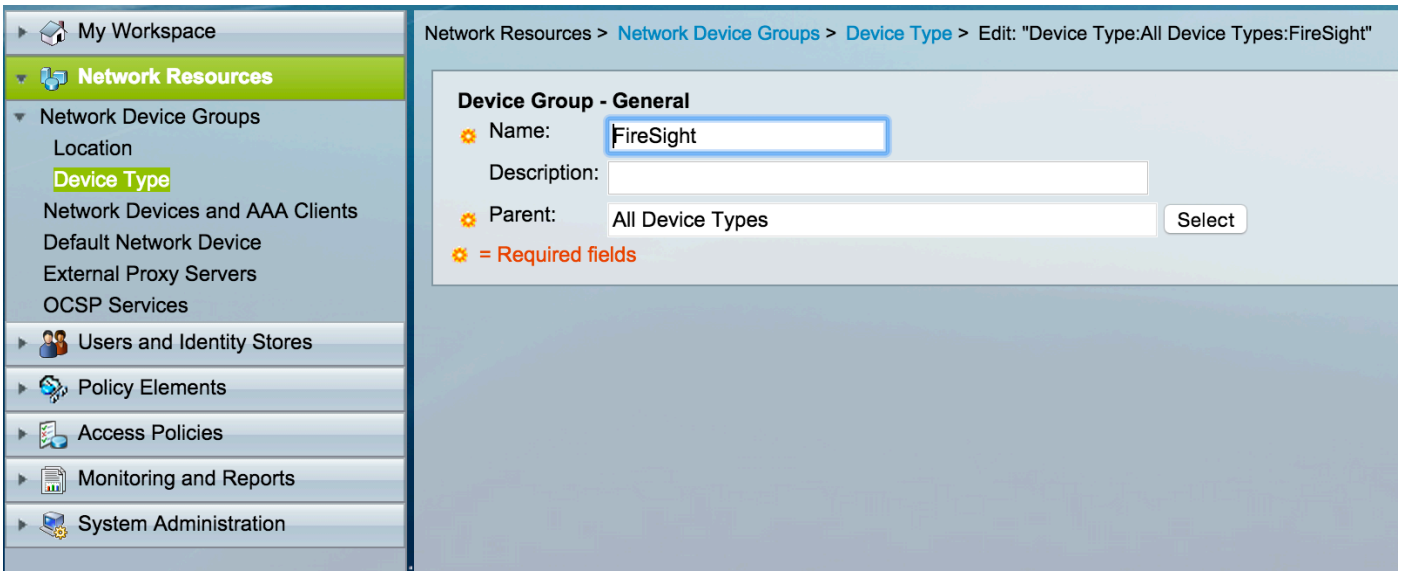
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Configuración

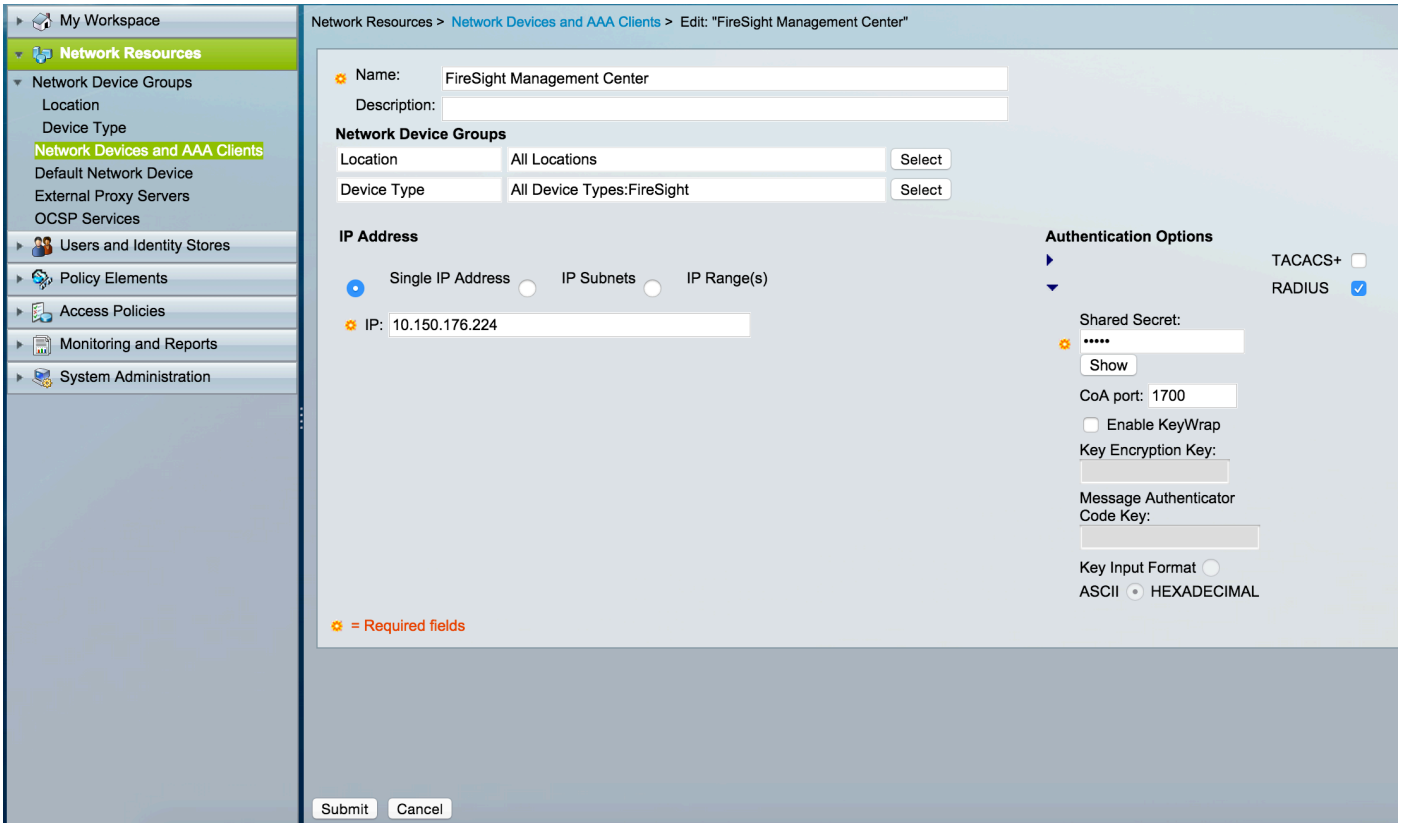
configuración de ACS 5.x

Configuración de dispositivos de red y grupos de dispositivos de red

- Desde la GUI de ACS, navegue hasta Network Device Group, haga clic en Device Type y cree un Device Group. En la siguiente captura de pantalla de ejemplo, se ha configurado el tipo de dispositivo FireSight. En un paso posterior, se hará referencia a este tipo de dispositivo en la definición de regla de directiva de autorización. Click Save.



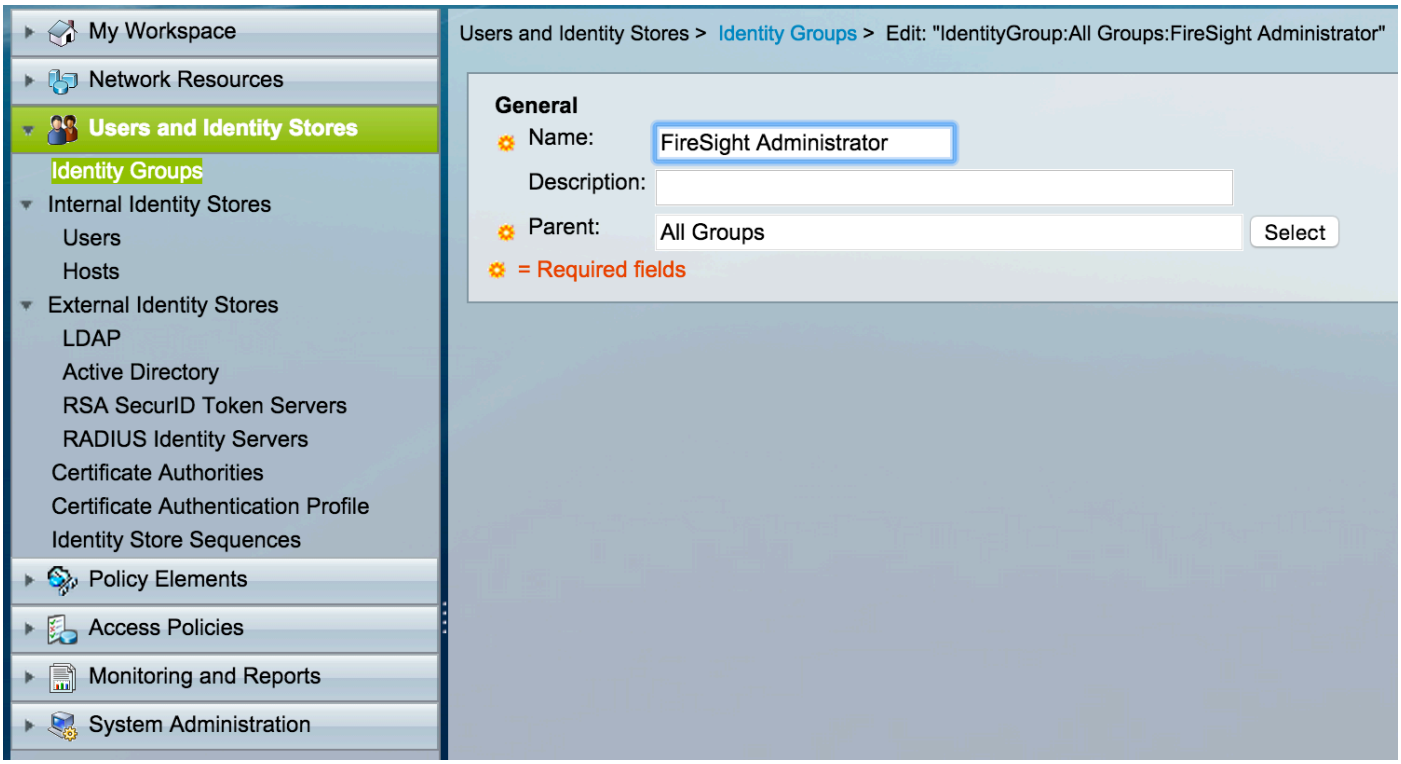
- Desde la GUI de ACS, navegue hasta Network Device Group, haga clic en Network Devices and AAA clients y agregue un dispositivo. Proporcione un nombre descriptivo y una dirección IP del dispositivo. El FireSIGHT Management Center se define en el siguiente ejemplo.



- En Network Device Groups, configure Device Type igual que el grupo de dispositivos creado en el paso anterior.
- Marque la casilla de verificación junto a Opciones de autenticación, seleccione la casilla de verificación RADIUS e ingrese la clave secreta compartida que se utilizará para este NAD. Tenga en cuenta que la misma clave secreta compartida se utilizará de nuevo más adelante cuando configure el servidor RADIUS en FireSIGHT Management Center. Para revisar el valor de la tecla de texto sin formato, haga clic en el botón Show. Haga clic en Submit (Enviar).
- Repita los pasos anteriores para todos los FireSIGHT Management Centers y dispositivos administrados que requieran autenticación/autorización de usuario RADIUS para el acceso a la interfaz gráfica de usuario o al shell.

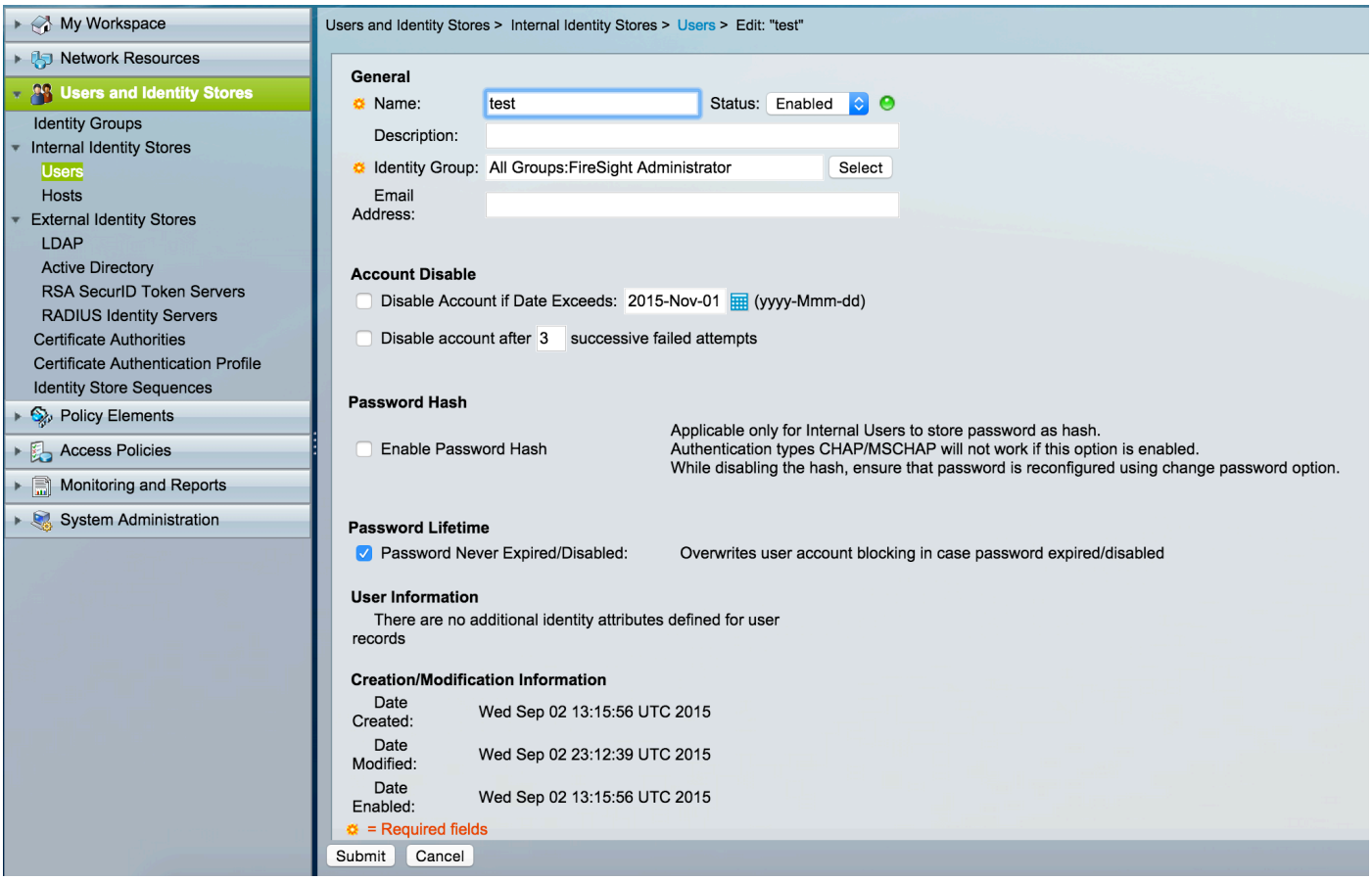
Adición de un Grupo de Identidad en ACS

- Navegue hasta Usuarios y almacenes de identidad, configure Grupo de identidad. En este ejemplo, el grupo de identidad creado es "FireSight Administrator". Este grupo se vinculará al perfil de autorización definido en los pasos siguientes.



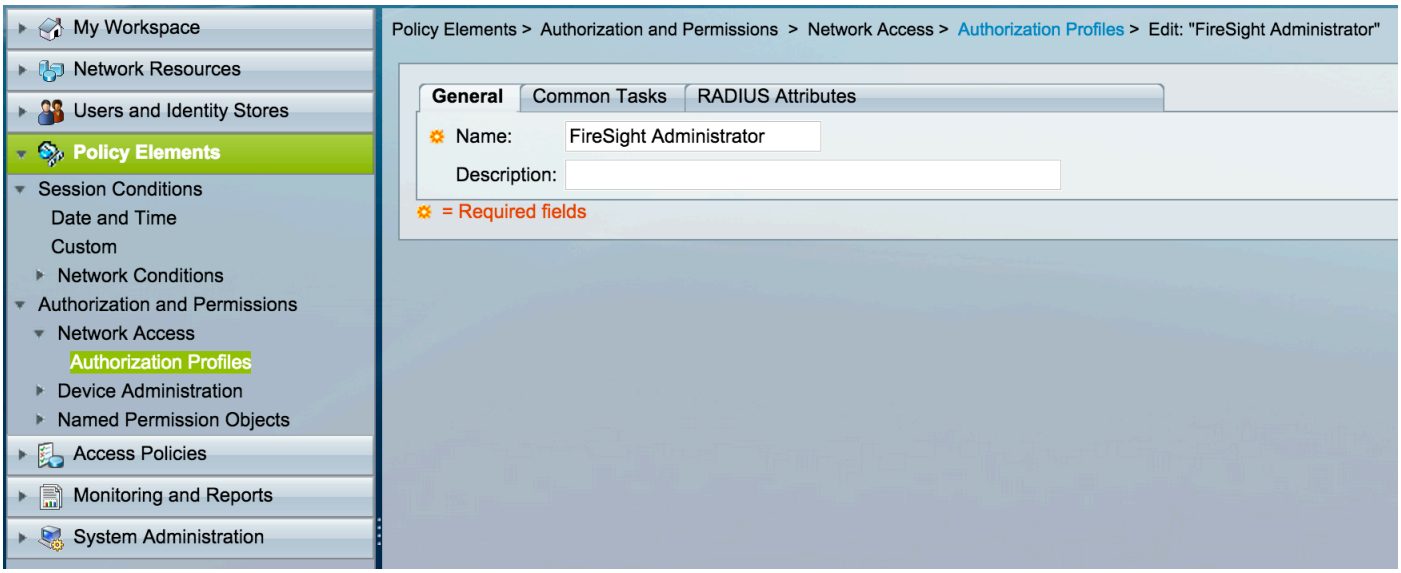
Adición de un Usuario Local a ACS

- Vaya a la sección Usuarios y almacenes de identidad, configurar Usuarios en Almacenes de identidad internos. Introduzca la información necesaria para la creación de usuarios locales, seleccione el grupo de identidad creado en el paso anterior y haga clic en Enviar.

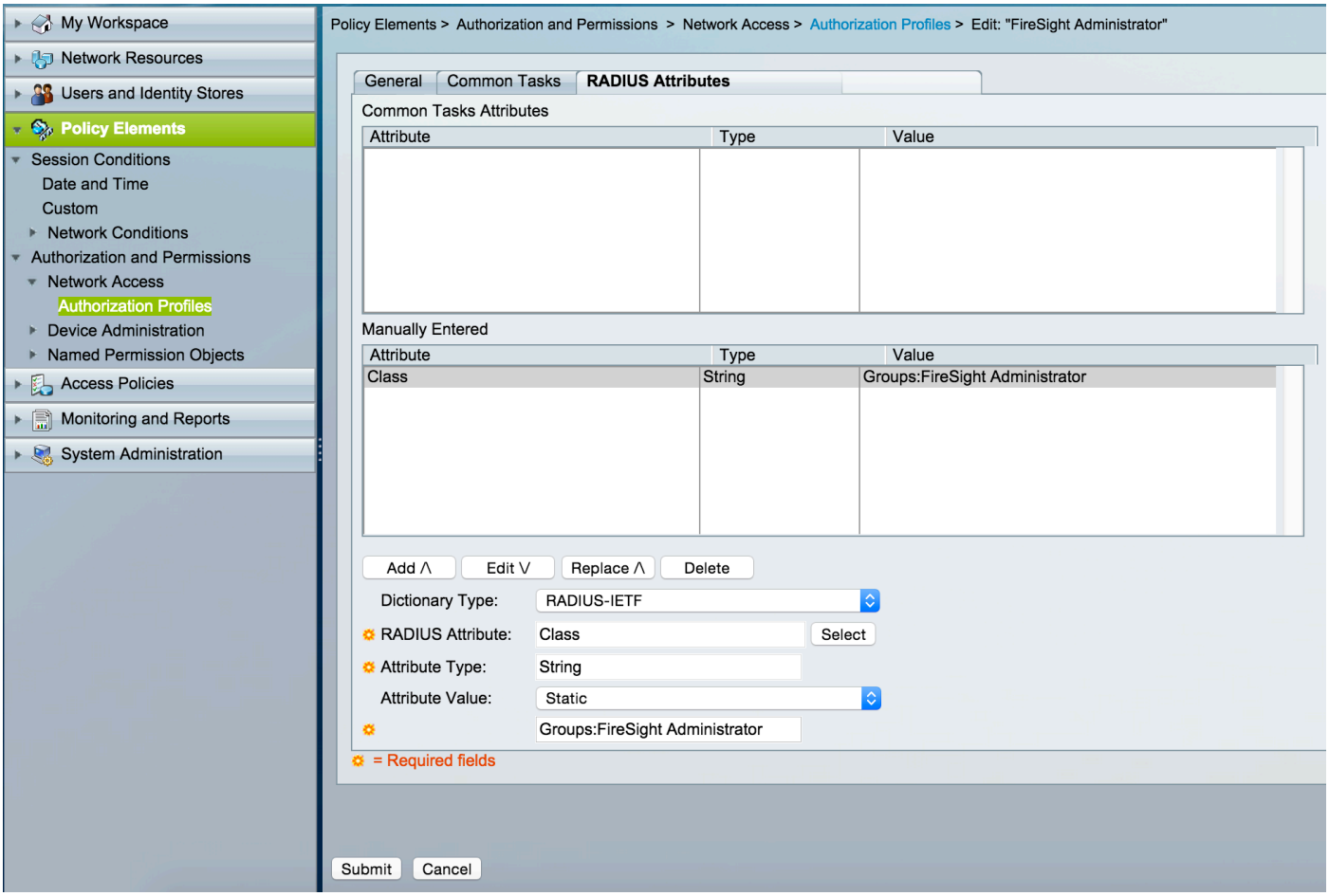


Configuración de la política ACS

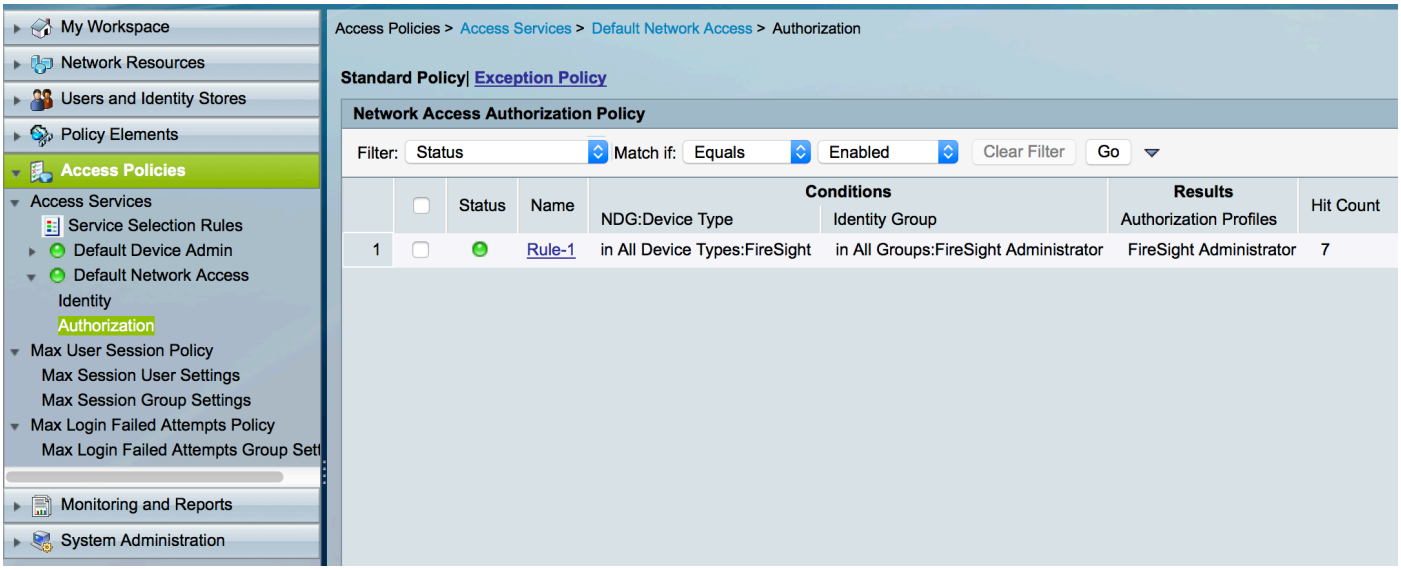
- En la GUI de ACS, navegue hasta Elementos de política > Autorización y permisos > Acceso a la red > Perfiles de autorización. Cree un nuevo perfil de autorización con un nombre descriptivo. En el ejemplo siguiente, la política creada es FireSight Administrator.



- En la pestaña RADIUS attributes, agregue un atributo manual para autorizar el grupo de identidad creado anteriormente y haga clic en Submit .



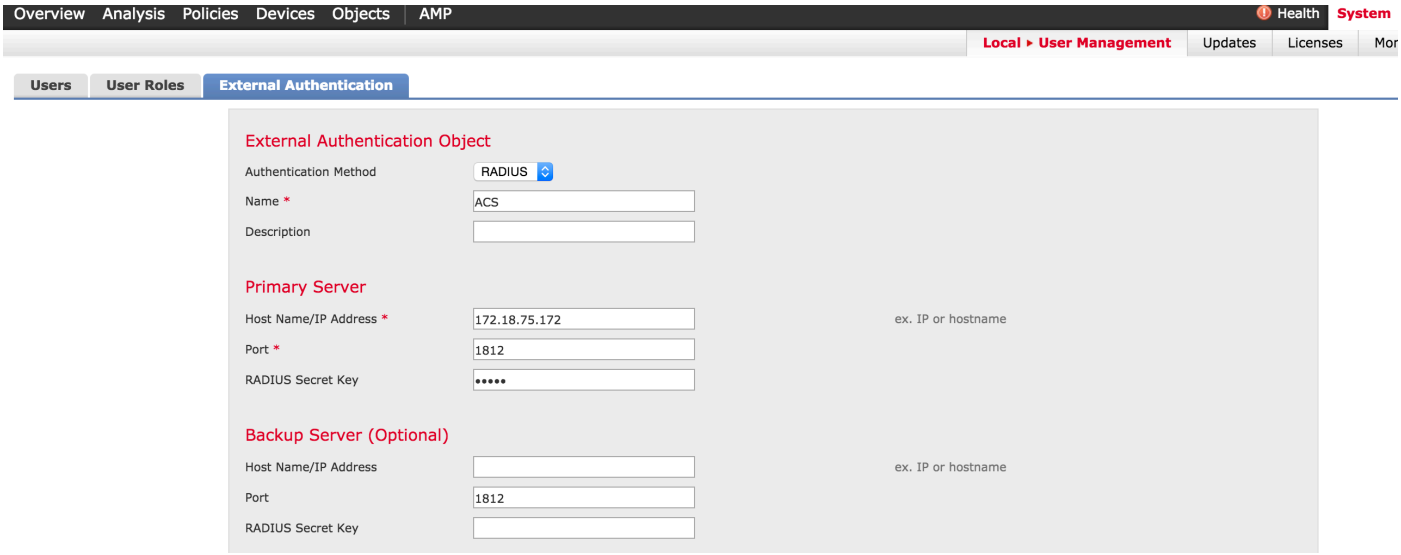
- Vaya a Access Policies > Access Services > Default Network Access > Authorization y configure una nueva política de autorización para las sesiones de administración de FireSight Management Center. El siguiente ejemplo utiliza la condición NDG:Device Type & Identity Group para hacer coincidir el tipo de dispositivo y el grupo de identidad configurados en los pasos anteriores.
- A continuación, esta política se asocia al perfil de autorización del administrador de FireSight configurado anteriormente como Resultado. Haga clic en Submit (Enviar).



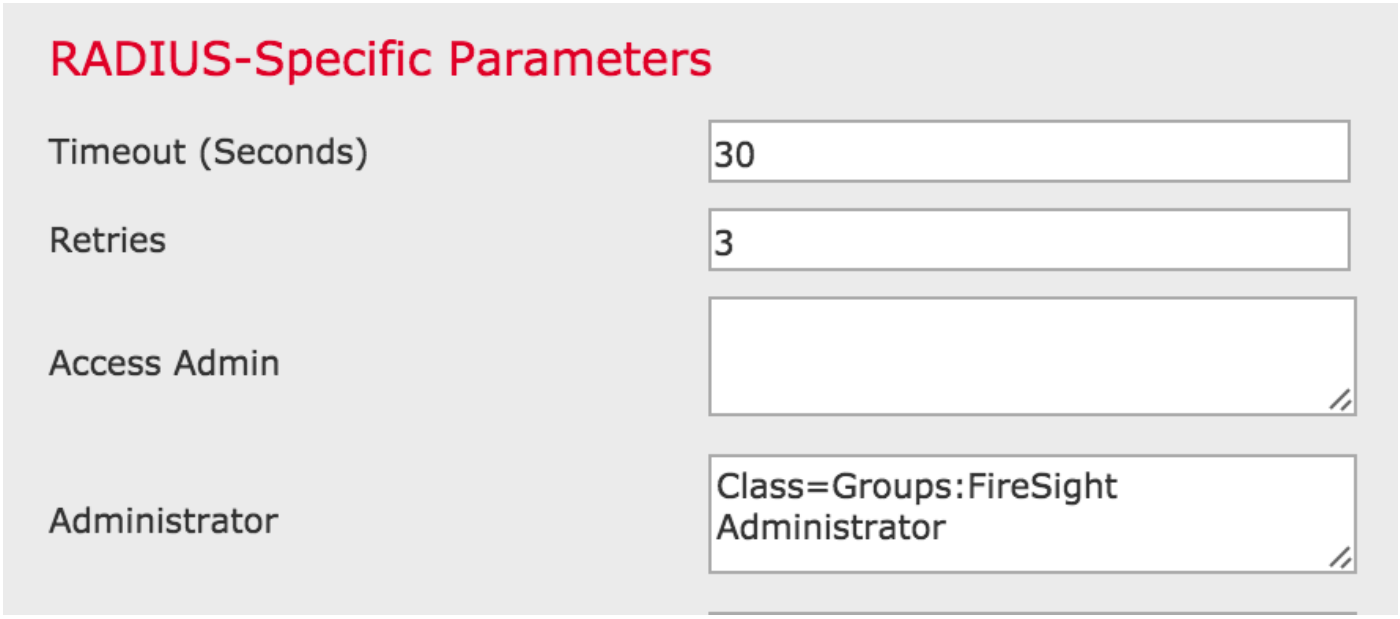
Configuración de FireSight Management Center

Configuración de políticas del sistema FireSight Manager

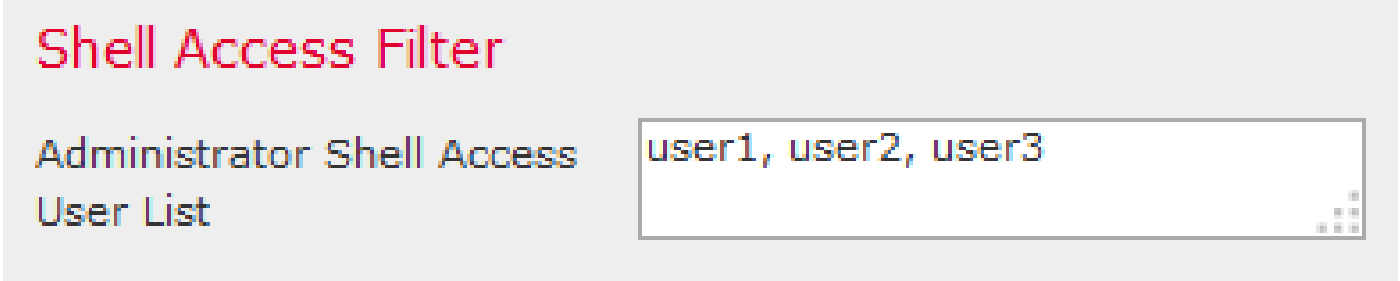
- Inicie sesión en FireSIGHT MC y navegue hasta System > Local > User Management. Haga clic en la pestaña Autenticación Externa. Haga clic en el botón + Create Authentication Object para agregar un nuevo servidor RADIUS para la autenticación/autorización de usuario.
- Seleccione RADIUS para el Método de autenticación. Introduzca un nombre descriptivo para el servidor RADIUS. Introduzca el nombre de host/dirección IP y la clave secreta RADIUS. La clave secreta debe coincidir con la clave previamente configurada en ACS. Opcionalmente, ingrese una copia de seguridad del nombre de host/dirección IP del servidor ACS si existe.



- En la sección Parámetros específicos de RADIUS, en este ejemplo, el valor Class=Groups:FireSight Administrator se asigna al grupo FireSight Administrator. Este es el valor que ACS devuelve como parte de ACCESS-ACCEPT. Haga clic en Save para guardar la configuración o continúe con la sección Verify a continuación para probar la autenticación con ACS.



- En Shell Access Filter, ingrese una lista de usuarios separada por comas para restringir las sesiones de shell/SSH.



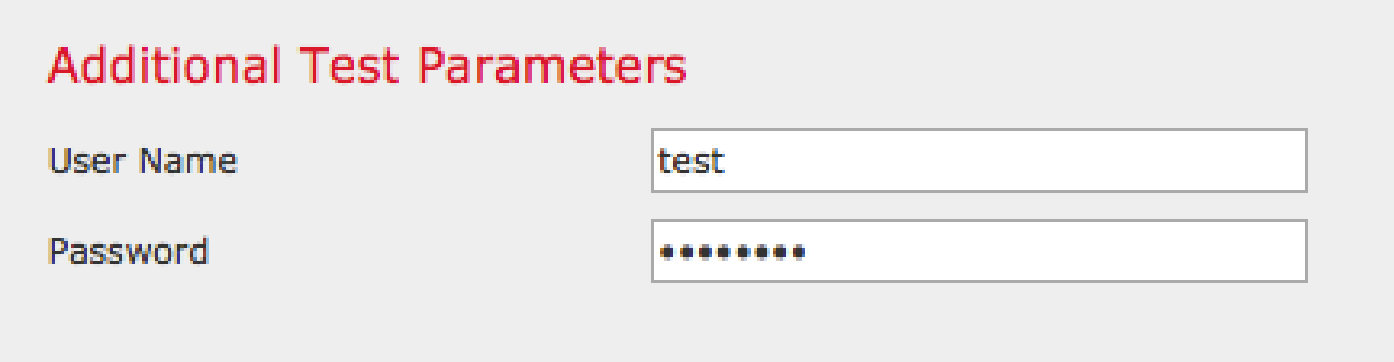
Habilitar autenticación externa

Por último, complete estos pasos para habilitar la autenticación externa en el FMC:

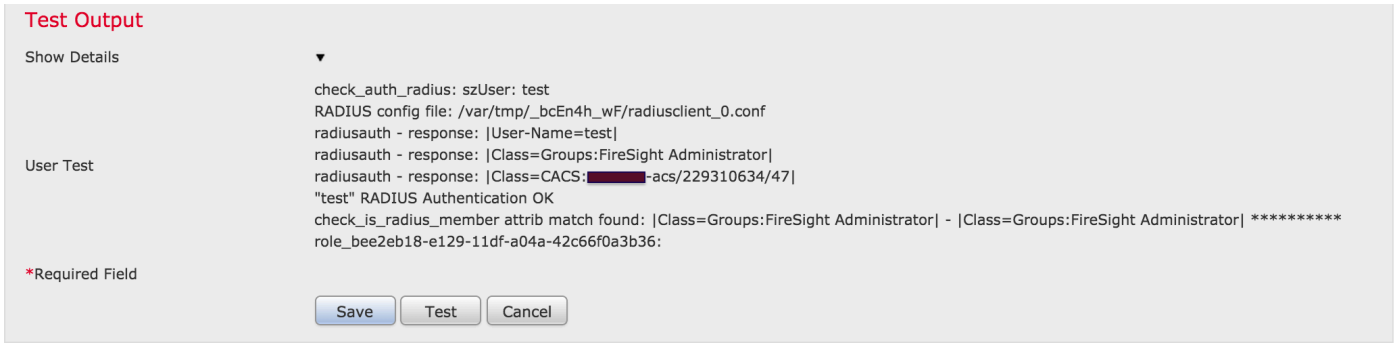
1. Vaya a System > Local > System Policy.
2. Seleccione External Authentication en el panel izquierdo.
3. Cambie el Estado a Activado (desactivado de forma predeterminada).
4. Habilite el servidor ACS RADIUS agregado.
5. Guarde la directiva y vuelva a aplicarla en el dispositivo.

Verificación

- Para probar la autenticación de usuario con ACS, desplácese hacia abajo hasta la sección Parámetros de prueba adicionales e ingrese un nombre de usuario y una contraseña para el usuario ACS. Haga clic en Test. Una prueba correcta dará como resultado un mensaje verde Éxito: prueba finalizada en la parte superior de la ventana del navegador.



- Para ver los resultados de la autenticación de prueba, vaya a la sección Test Output y haga clic en la flecha negra junto a Show Details. En la siguiente captura de pantalla de ejemplo, observe el "radiusauth - response: El valor de |Class=Groups:FireSight Administrator|" recibido de ACS. Debe coincidir con el valor de Class asociado con el grupo local de FireSight configurado en el MC de FireSIGHT anterior. Click Save.



Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).