Configuración de ThreatGrid RADIUS sobre autenticación DTLS para la consola y el portal OPadmin

Contenido

Introducción

Este documento describe la función de autenticación RADIUS (servicio de usuario de acceso telefónico de autenticación remota) introducida en la versión 2.10 de ThreatGrid (TG). Permite a los usuarios iniciar sesión en el portal de administración, así como en el portal de consola con las credenciales almacenadas en el servidor de autenticación, autorización y contabilidad (AAA).

En este documento encontrará los pasos necesarios para configurar la función.

Prerequisites

Requirements

- ThreatGrid versión 2.10 o superior
- Servidor AAA que admite la autenticación RADIUS sobre DTLS (draft-ietf-radext-dtls-04)

Componentes Utilizados

- Appliance ThreatGrid 2.10
- Identity Services Engine (ISE) 2.7

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

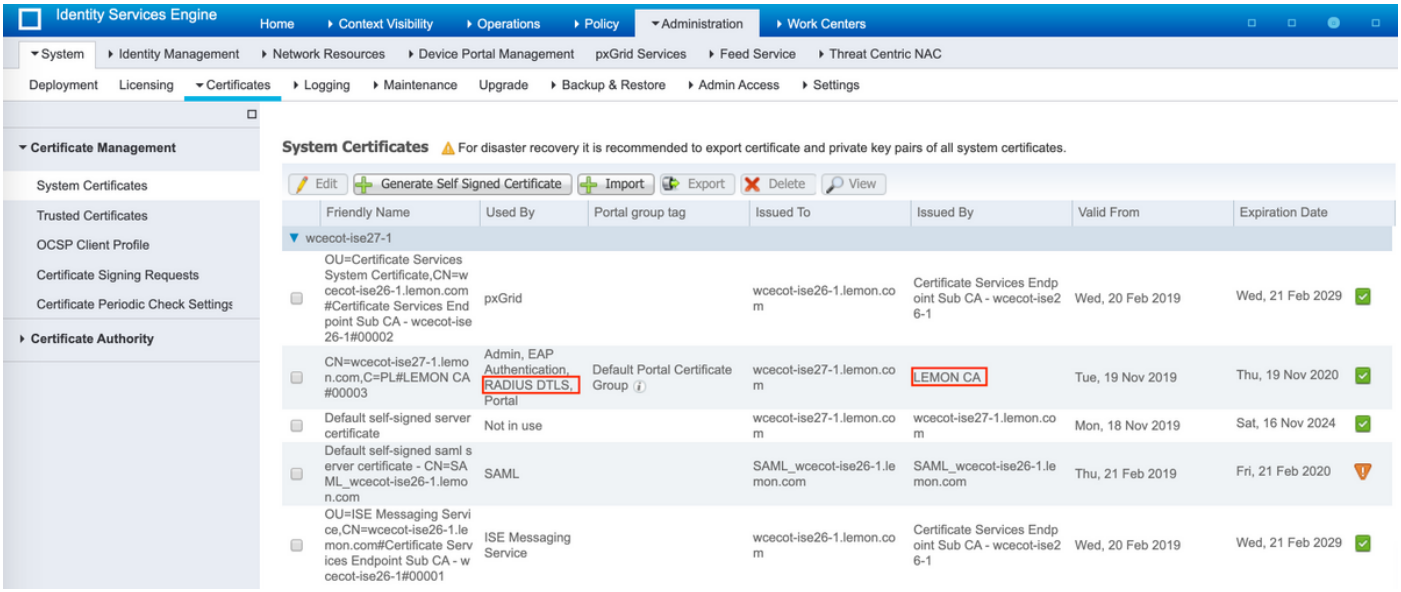
Esta sección proporciona instrucciones detalladas sobre cómo configurar ThreatGrid Appliance e ISE para la función de autenticación RADIUS.

Nota: Para configurar la autenticación, asegúrese de que se permite la comunicación en el puerto UDP 2083 entre la interfaz ThreatGrid Clean y el nodo de servicio de políticas de ISE (PSN).

Configuración

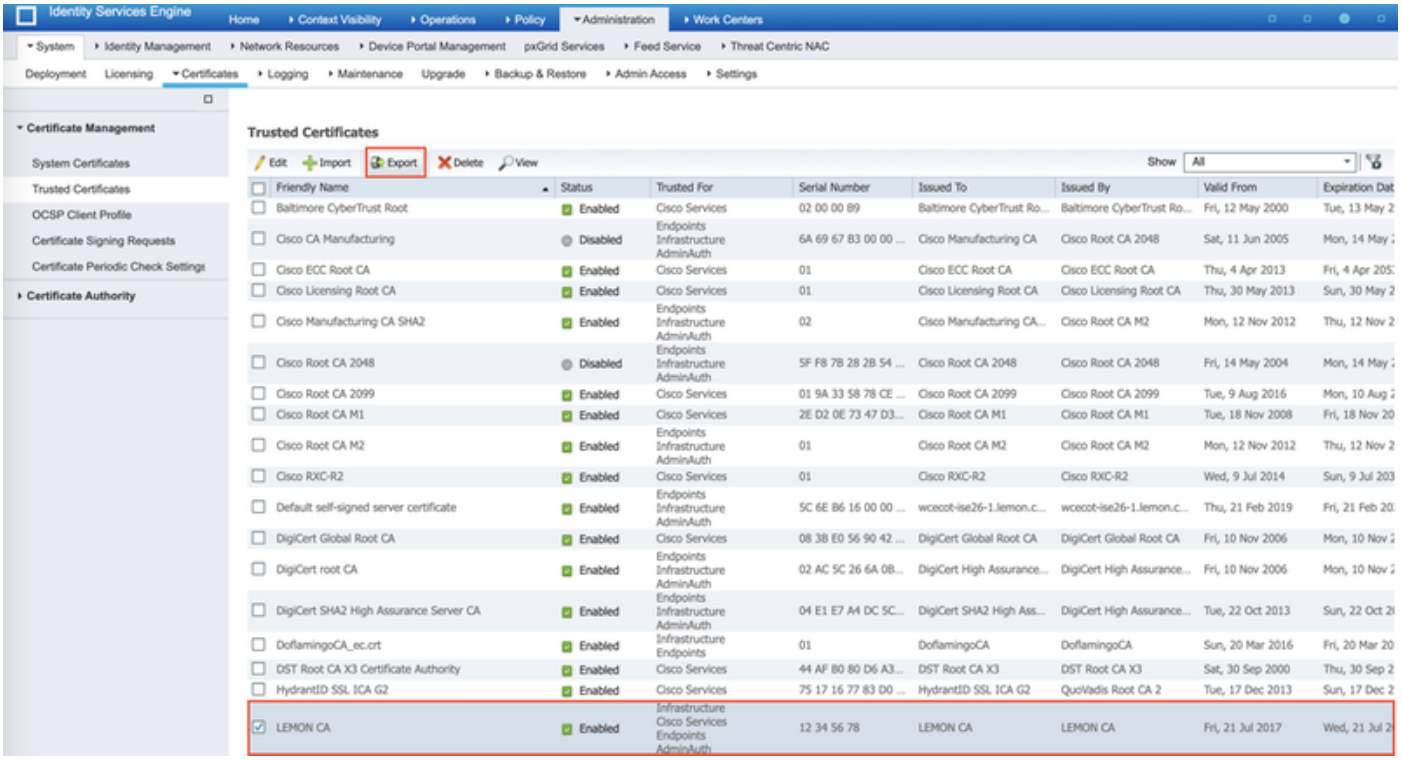
Paso 1. Preparar el certificado de ThreatGrid para la autenticación.

RADIUS sobre DTLS utiliza la autenticación de certificados mutua, lo que significa que se necesita el certificado de Autoridad de Certificación (CA) de ISE. Primero verifique qué certificado DTLS RADIUS firmado por CA:



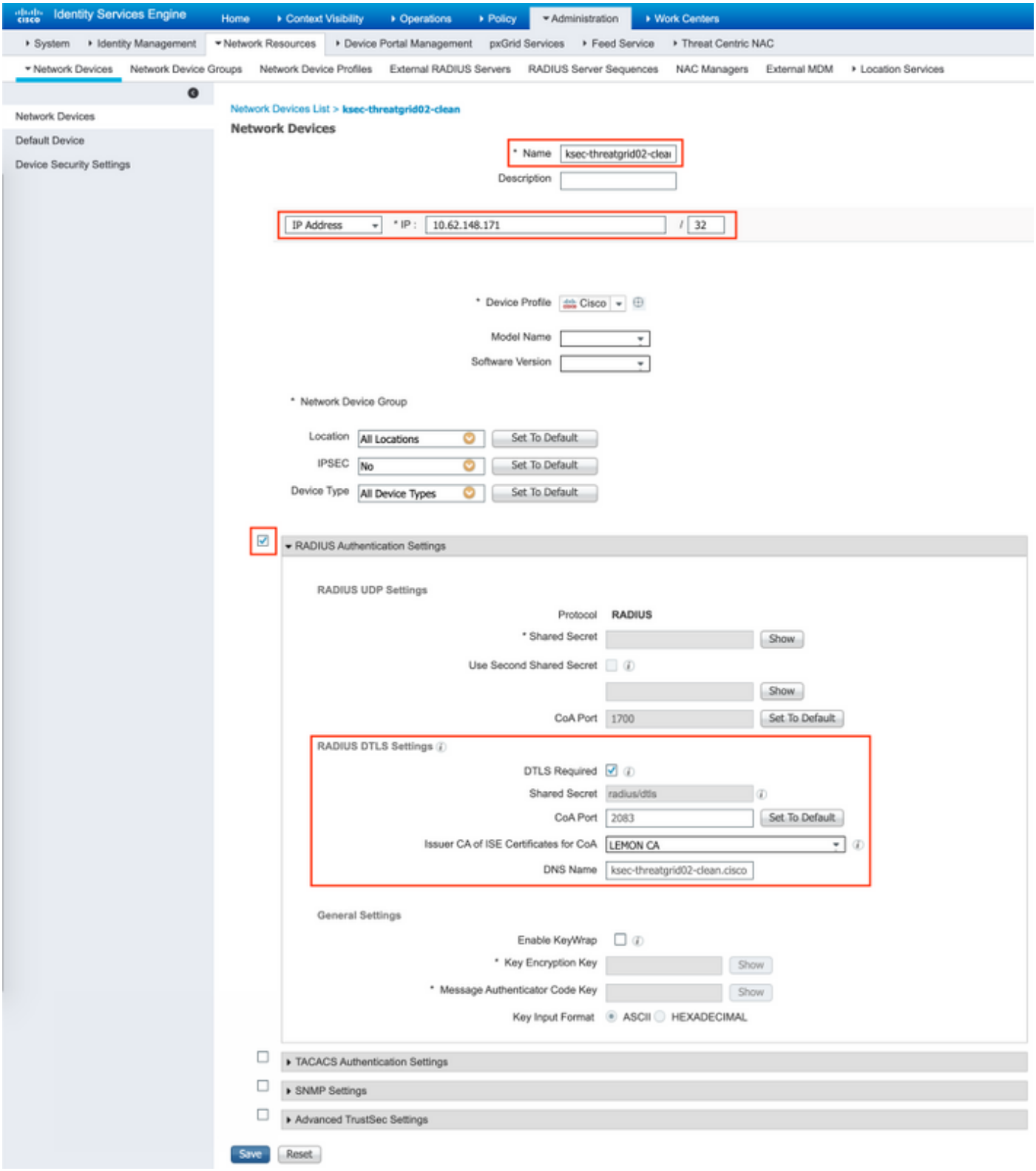
Paso 2. Exportar el certificado de CA de ISE.

Vaya a **Administration > System > Certificates > Certificate Management > Trusted Certificates**, localice la CA, seleccione **Export** como se muestra en la imagen y guarde el certificado en el disco para más adelante:



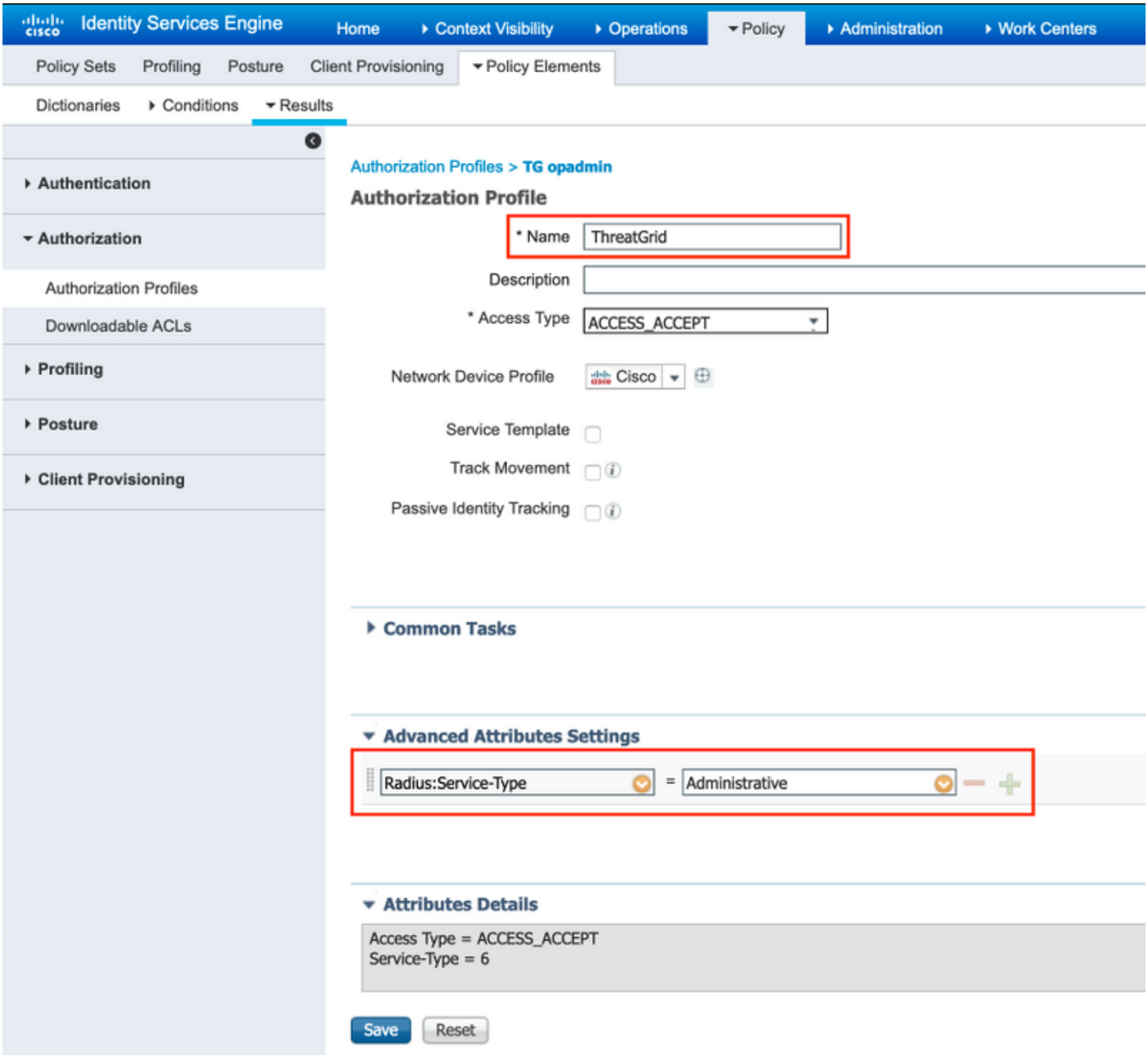
Paso 3. Agregue ThreatGrid como dispositivo de acceso a la red.

Vaya a **Administration > Network Resources > Network Devices > Add** para crear una nueva entrada para TG e introduzca el **Name**, la **dirección IP** de la interfaz Clean y seleccione **DTLS Required** como se muestra en la imagen. Haga clic en **Guardar** en la parte inferior:



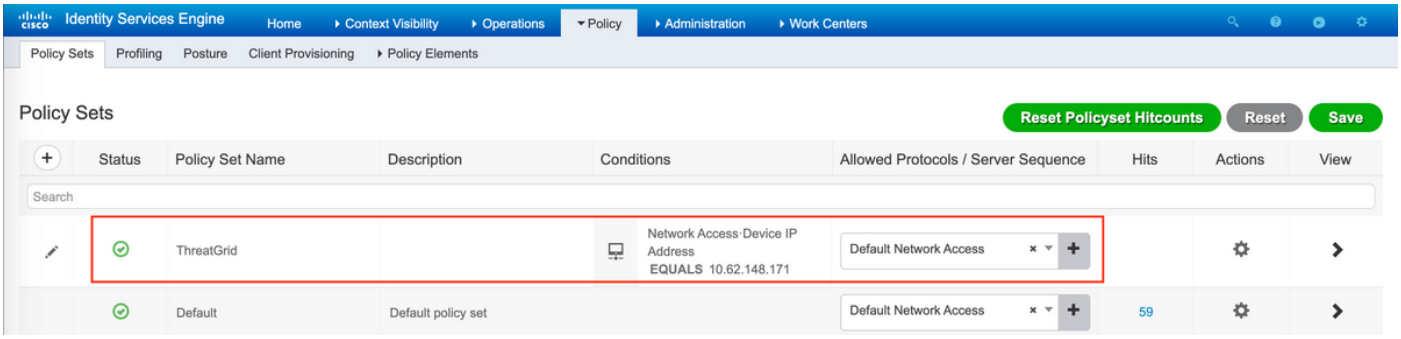
Paso 4. Cree un perfil de autorización para la política de autorización.

Navegue hasta **Política > Elementos de política > Resultados > Autorización > Perfiles de autorización** y haga clic en **Agregar**. Ingrese **Name** y seleccione **Advanced Attributes Settings** como se muestra en la imagen y haga clic en **Save**:



Paso 5. Cree una política de autenticación.

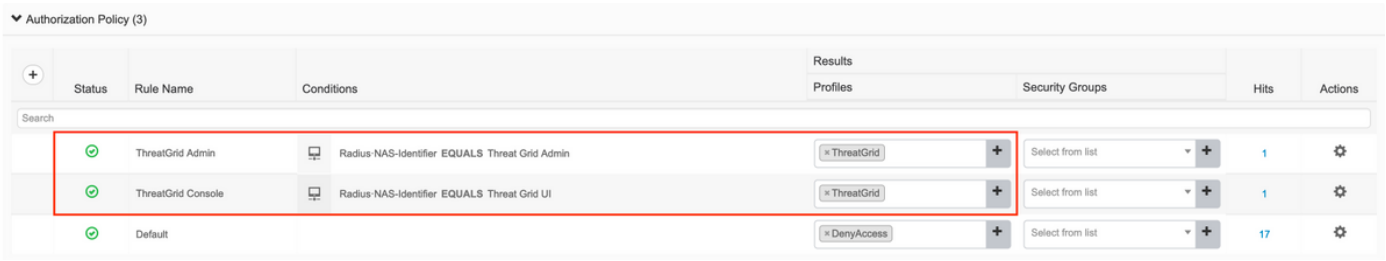
Navegue hasta **Política > Conjuntos de Políticas** y haga clic en "**+**". Ingrese Policy Set **Name** y establezca la condición en **NAD IP Address**, asignada a la interfaz limpia de TG, haga clic en **Save** como se muestra en la imagen:



Paso 6. Cree una política de autorización.

Haga clic en el botón "**>**" para ir a la política de autorización, expanda la política de autorización,

haga clic en "**+**" y configure como se muestra en la imagen, después de finalizar, haga clic en **Guardar**:



> **Sugerencia**: puede crear una regla de autorización para todos los usuarios que coincidan con ambas condiciones, Admin y UI.

Paso 7. Cree un certificado de identidad para ThreatGrid.

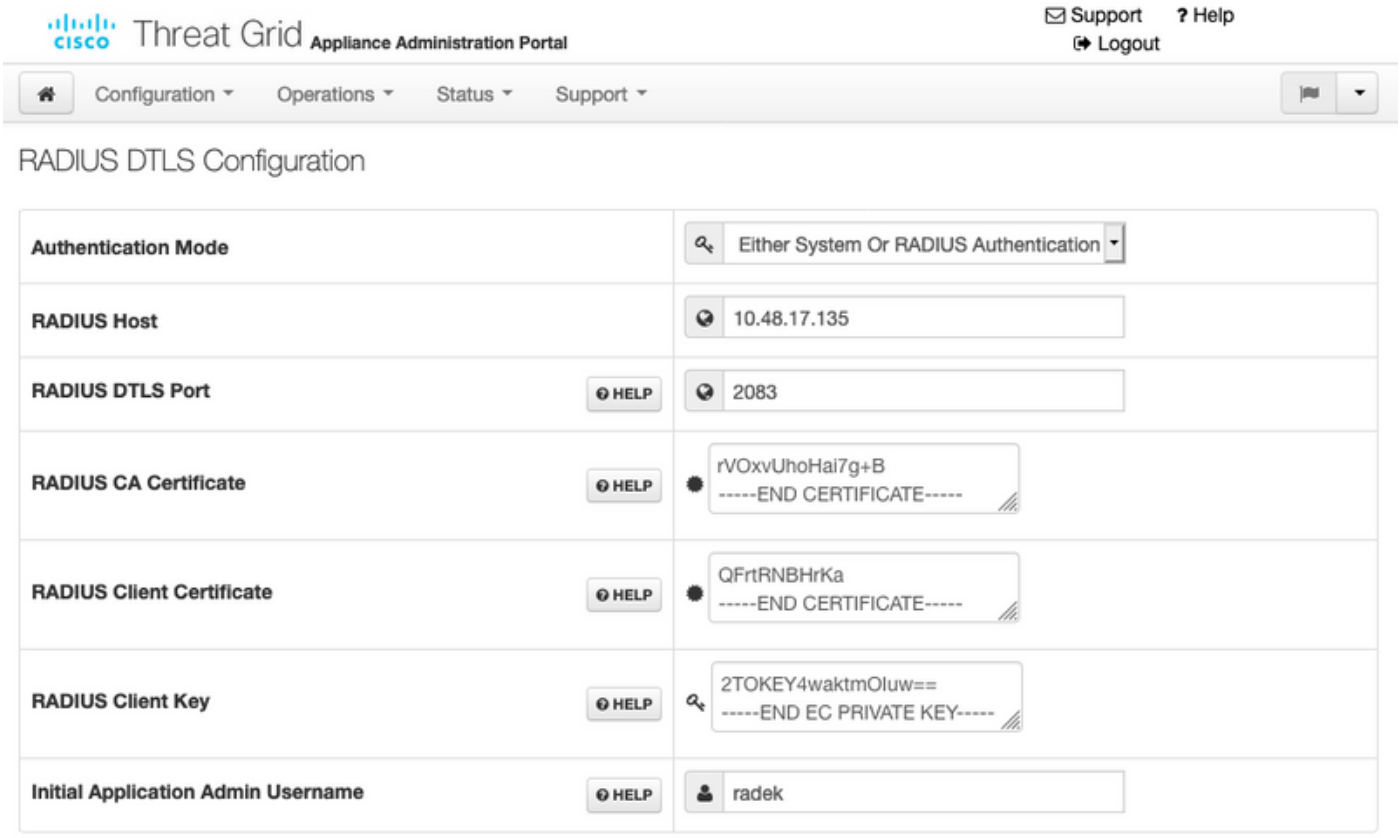
El certificado de cliente de ThreatGrid debe basarse en la clave de curva elíptica:

```
openssl ecparam -name secp521r1 -genkey -out private-ec-key.pem
```

Debe estar firmado por la CA en la que confía ISE. Marque *Importar los certificados raíz a la* página *almacén de certificados de confianza* para obtener más información sobre cómo agregar el certificado de CA al almacén de certificados de confianza de ISE.

Paso 8. Configure ThreatGrid para utilizar RADIUS.

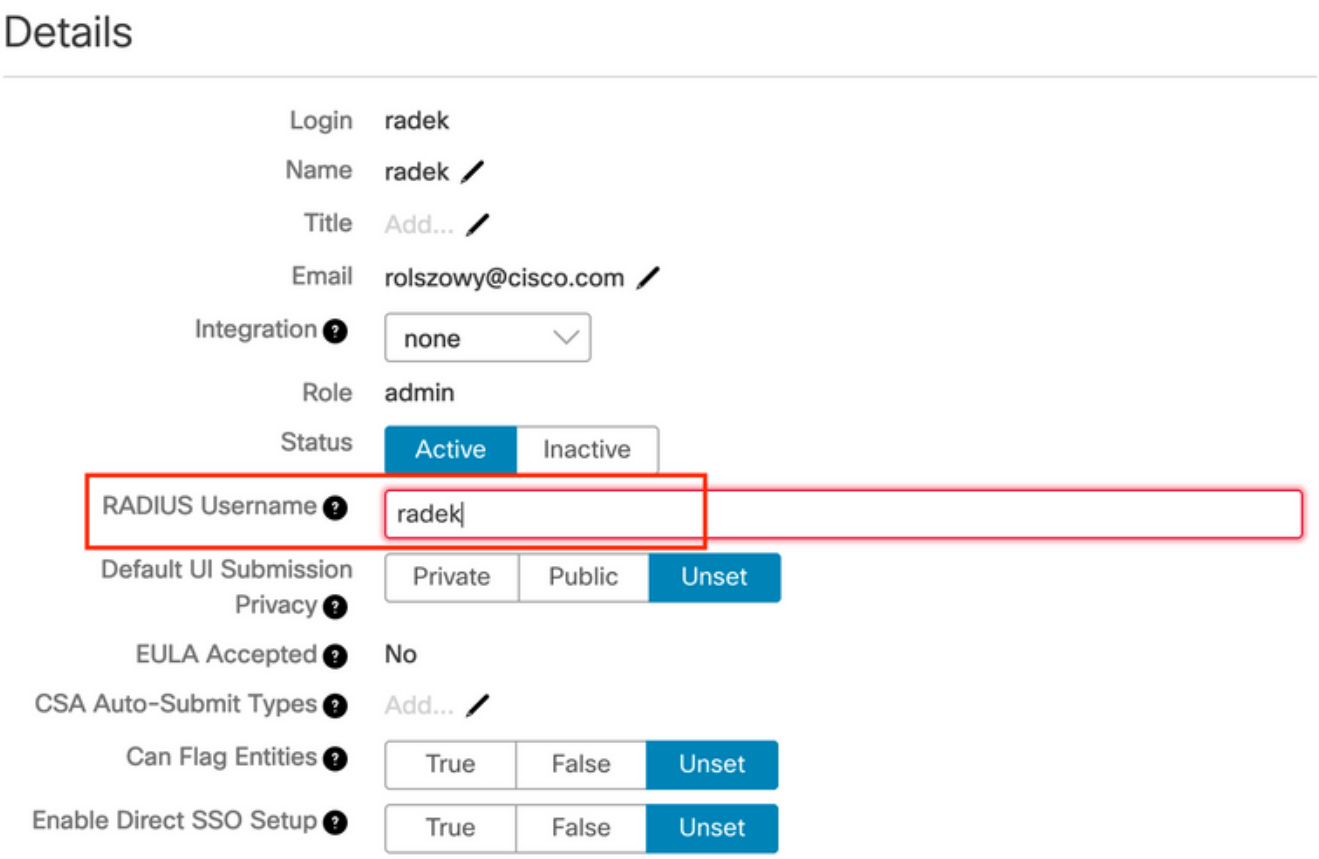
Inicie sesión en el portal de administración, navegue hasta **Configuration>RADIUS**. En RADIUS CA Certificate , pegue el contenido del archivo PEM recolectado de ISE, en Client Certificate pegue el certificado con formato PEM recibido de CA y en Client Key pegue el contenido del archivo private-ec-key.pem del paso anterior, como se muestra en la imagen. Haga clic en Save (Guardar):



Nota: Debe volver a configurar el dispositivo TG después de guardar la configuración RADIUS.

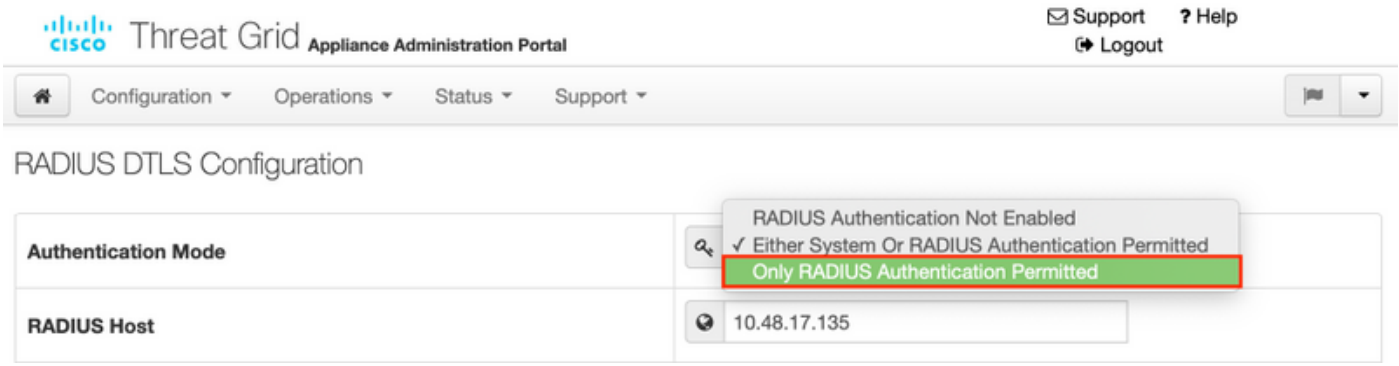
Paso 9. Agregue el nombre de usuario RADIUS a los usuarios de la consola.

Para iniciar sesión en el portal de la consola, debe agregar el atributo RADIUS Username al usuario respectivo como se muestra en la imagen:



Paso 10. Habilite la autenticación sólo RADIUS.

Después de iniciar sesión correctamente en el portal de administración, aparece una nueva opción, que desactiva completamente la autenticación del sistema local y deja el único basado en RADIUS.



Verificación

Una vez reconfigurado TG, cierre la sesión y ahora las páginas de inicio de sesión se ven como en las imágenes, el administrador y el portal de consola respectivamente:

Authentication Required

Authenticate using RADIUS:

RADIUS Login

RADIUS Password

Authenticate

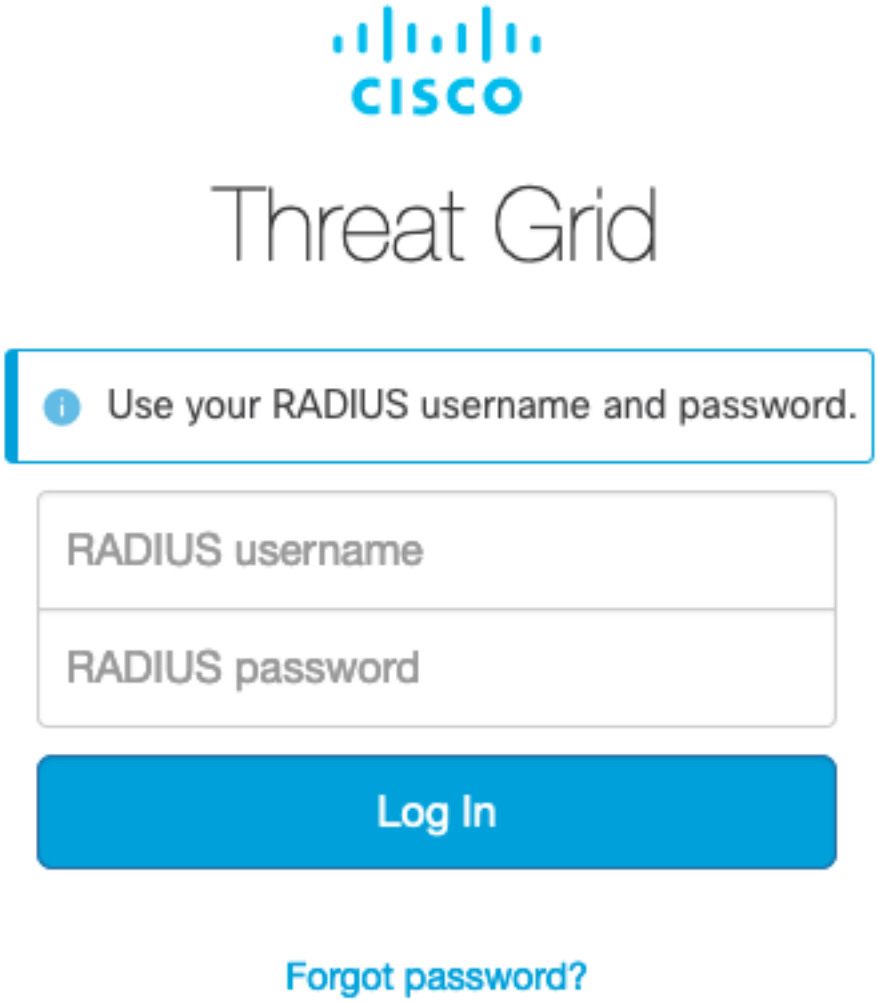
or

Authenticate using System Password:

System Password

Authenticate

This site is best viewed in: Internet Explorer 10+, Firefox 14+, Safari 6+, or Chrome 20+

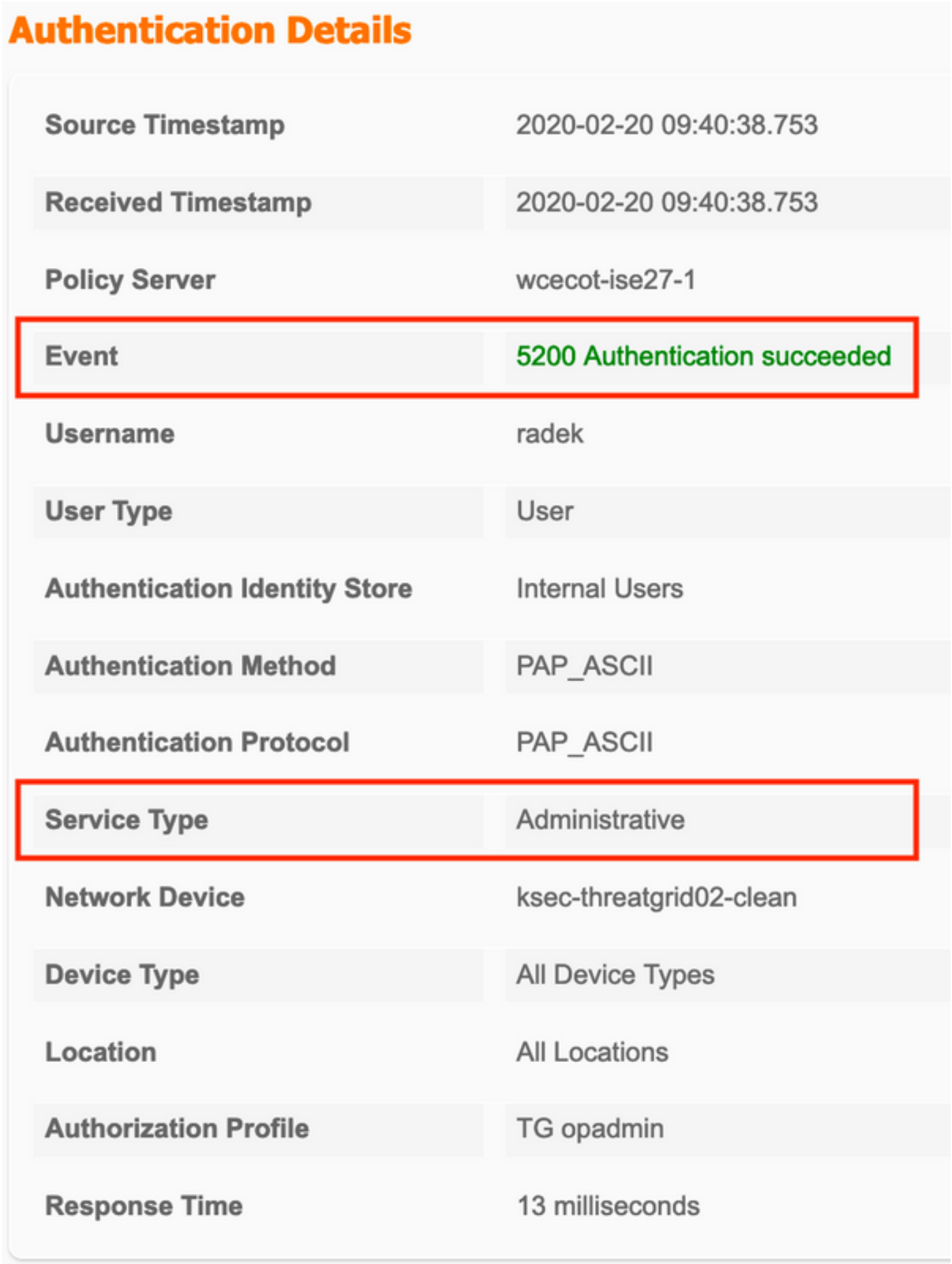


Troubleshoot

Hay tres componentes que podrían causar problemas: ISE, conectividad de red y ThreatGrid.

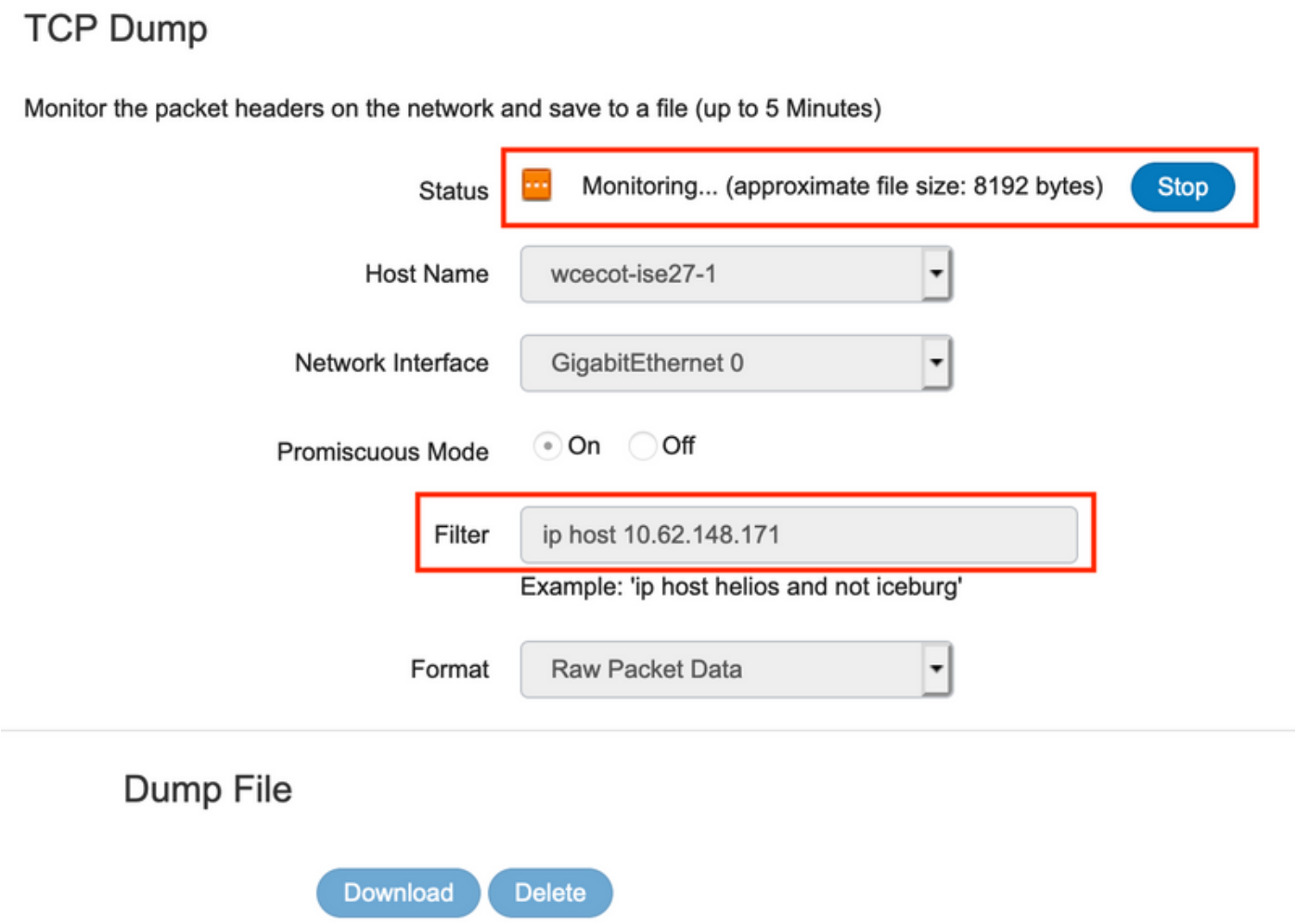
- En ISE, asegúrese de devolver ServiceType=Administrative a ThreatGrid las solicitudes de autenticación. Navegue hasta **Operaciones > RADIUS > Registros en Directo** en ISE y verifique los detalles:

Time	Status	Details	Repeat ...	Identity	Authentication Policy	Authorization Policy	Authorizati...	Network Device
×				Identity	ThreatGrid ×	Authorization Policy	Authorization	Network Device
Feb 20, 2020 09:40:38.753 AM	✓			radek	ThreatGrid >> Default	ThreatGrid >> ThreatGrid Admin	TG opadmin	ksec-threatgrid02-clean
Feb 20, 2020 09:40:18.260 AM	✓			radek	ThreatGrid >> Default	ThreatGrid >> ThreatGrid Console	TG console	ksec-threatgrid02-clean



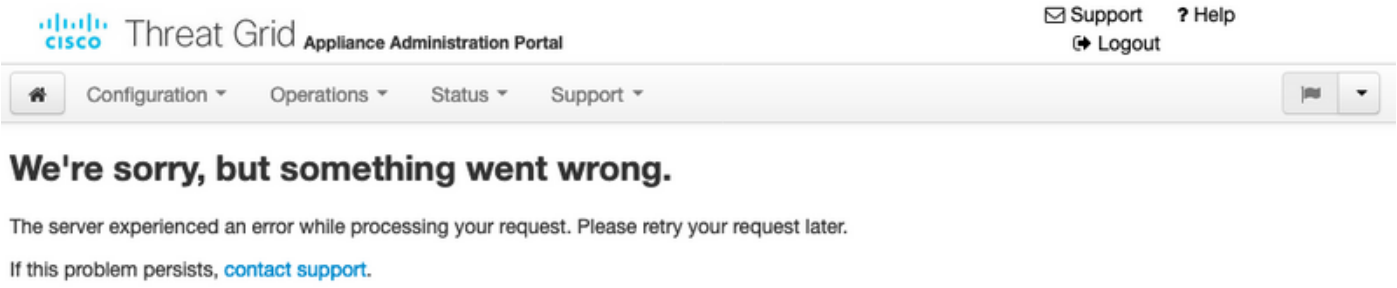
- Si no ve estas solicitudes, realice una captura de paquetes en ISE. Navegue hasta Operaciones >Solución de problemas **>Herramientas de diagnóstico> TCP Dump**, proporcione la IP en el campo Filtro de la interfaz de limpieza de TG, haga clic en **Inicio** e

intente iniciar sesión en ThreatGrid:



Debe ver que el número de bytes aumentó. Abra el archivo pcap en Wireshark para obtener más información.

- Si aparece el error "Lo sentimos, pero algo salió mal" después de hacer clic en Guardar en ThreatGrid y la página se muestra de la siguiente manera:



Esto significa que lo más probable es que haya utilizado la clave RSA para el certificado de cliente. Debe utilizar la clave ECC con los parámetros especificados en el paso 7.