# Konfigurieren von ThreatGrid RADIUS über DTLS-Authentifizierung für Konsole und OPadmin-Portal

## Inhalt



## Einführung

Dieses Dokument beschreibt die Authentifizierungsfunktion RADIUS (Remote Authentication Dial In User Service), die in ThreatGrid (TG), Version 2.10, eingeführt wurde. Benutzer können sich sowohl beim Admin-Portal als auch im Konsolenportal anmelden. Die Anmeldeinformationen werden im Authentication, Authorization and Accounting (AAA)-Server gespeichert.

In diesem Dokument finden Sie die notwendigen Schritte zum Konfigurieren der Funktion.

## Voraussetzungen

### Anforderungen

- ThreatGrid ab Version 2.10
- AAA-Server, der RADIUS über DTLS-Authentifizierung unterstützt (Draft-ietf-radext-dtls-04)

### Verwendete Komponenten

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konfigurieren

Dieser Abschnitt enthält detaillierte Anweisungen zur Konfiguration der ThreatGrid-Appliance und

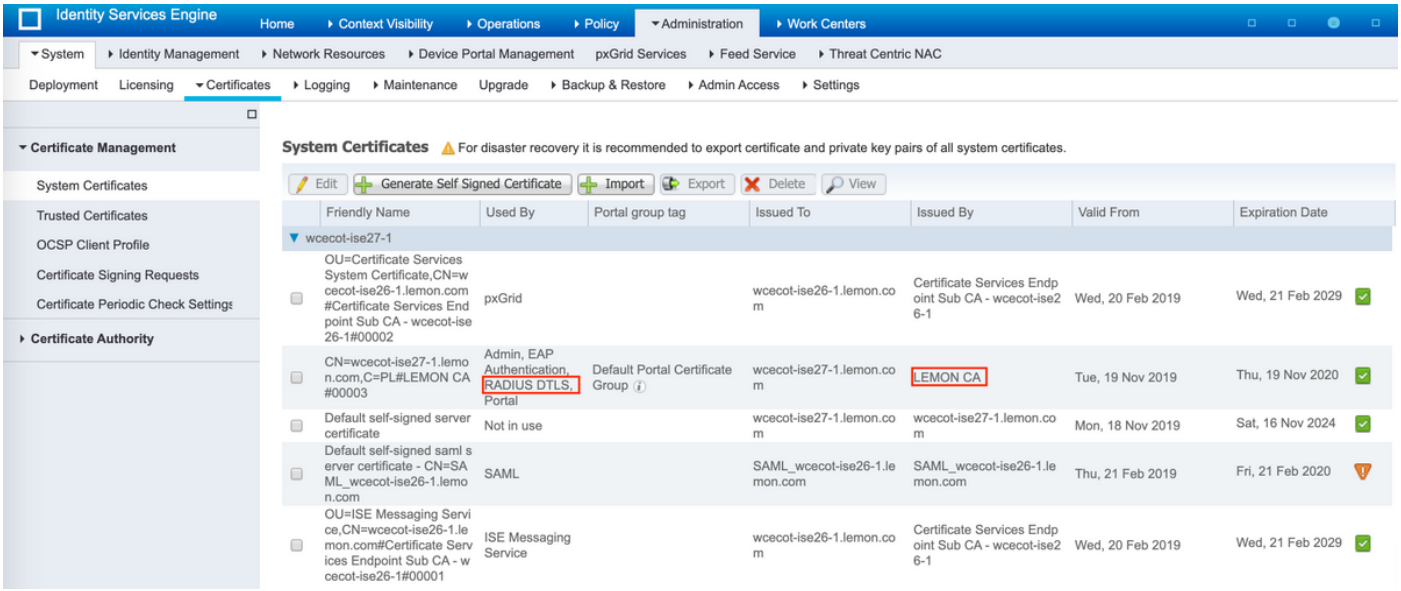
der ISE für die RADIUS-Authentifizierungsfunktion.

> **Hinweis**: Um die Authentifizierung zu konfigurieren, stellen Sie sicher, dass die Kommunikation zwischen ThreatGrid Clean-Schnittstelle und ISE Policy Service Node (PSN) auf Port UDP 2083 zulässig ist.

## Konfiguration

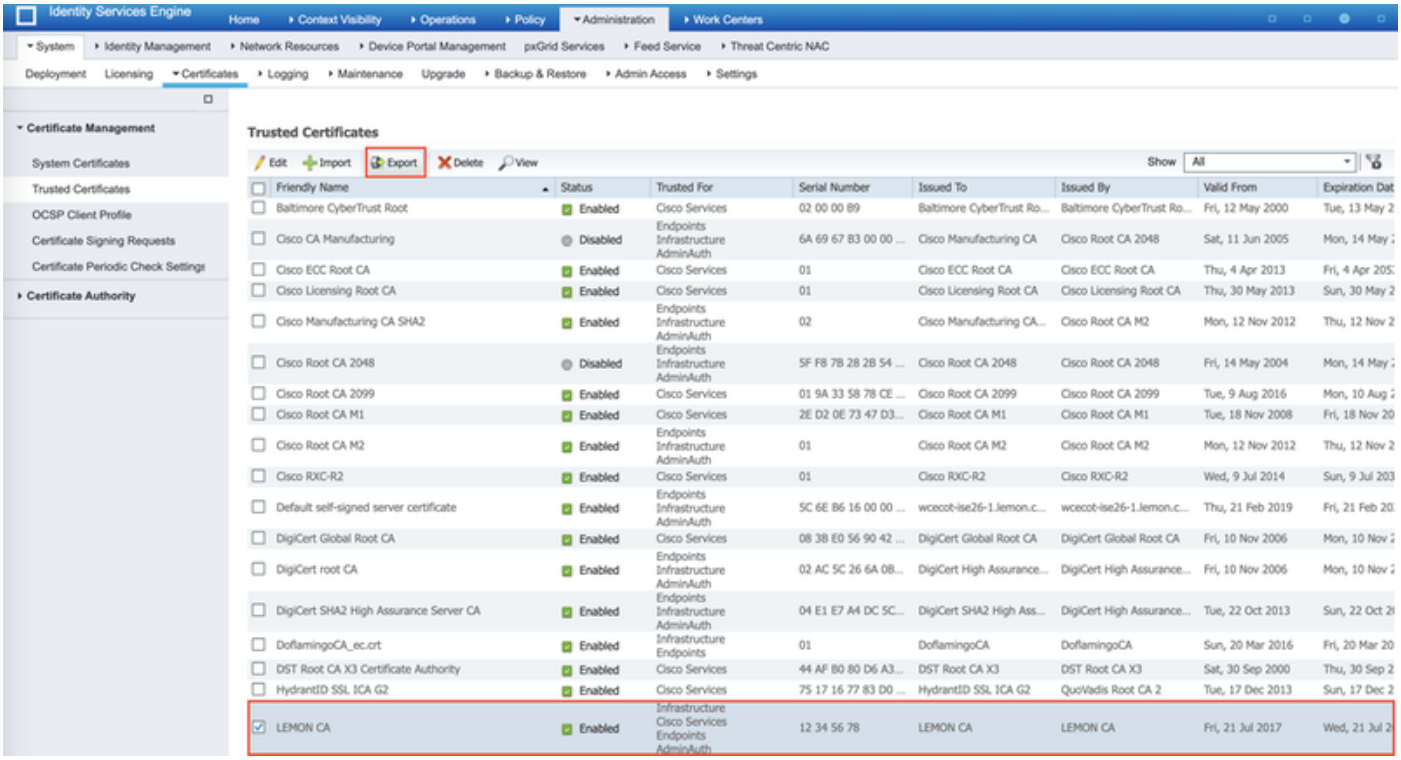
Schritt 1: Bereiten Sie das ThreatGrid-Zertifikat für die Authentifizierung vor.

RADIUS over DTLS verwendet gegenseitige Zertifikatsauthentifizierung, d. h. das Zertifikat der Zertifizierungsstelle (Certificate Authority, CA) von der ISE ist erforderlich. Überprüfen Sie zuerst, welches RADIUS DTLS-Zertifikat von der CA signiert wurde:



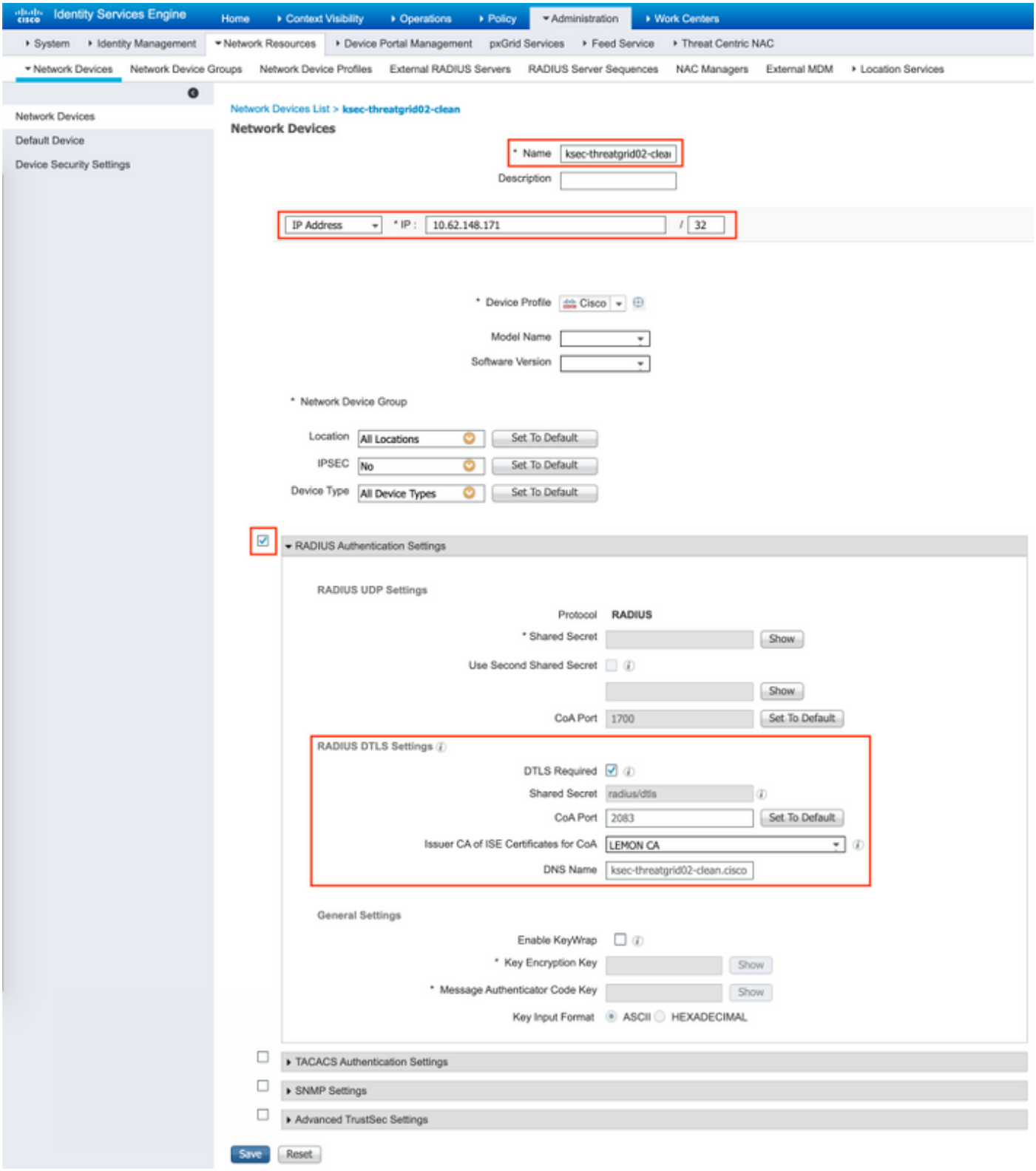

Schritt 2: Exportieren Sie das Zertifizierungsstellenzertifikat von der ISE.

Navigieren Sie zu **Administration > System > Certificates > Certificate Management > Trusted Certificates**, suchen Sie die Zertifizierungsstelle, wählen Sie **Export (Exportieren)** aus, wie im Bild gezeigt, und speichern Sie das Zertifikat zu einem späteren Zeitpunkt auf dem Datenträger:



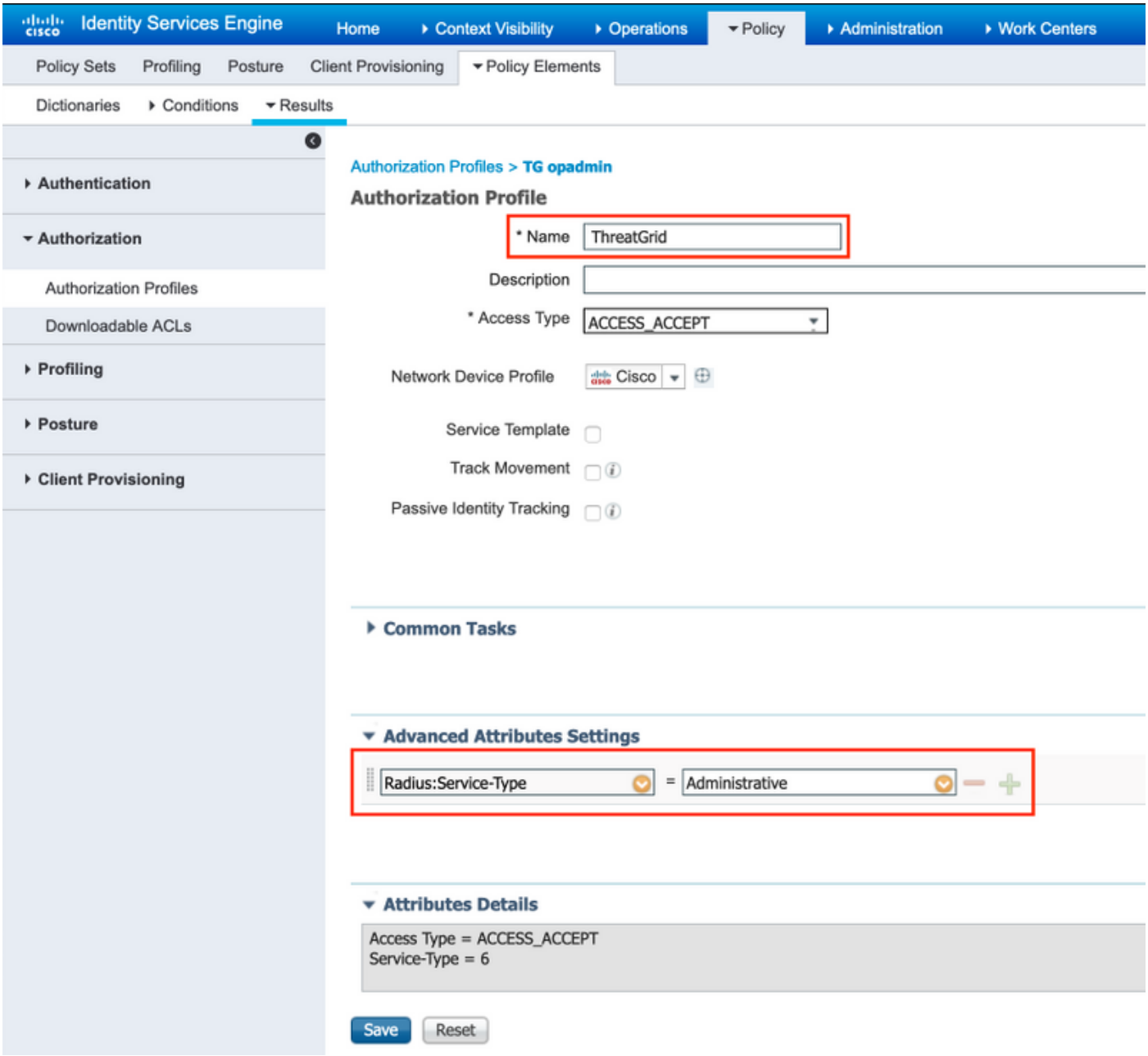

Schritt 3: Hinzufügen von ThreatGrid als Netzwerkzugriffsgerät

Navigieren Sie zu **Administration > Network Resources > Network Devices > Add**, um einen neuen Eintrag für TG zu erstellen, und geben Sie den **Namen**, die **IP-Adresse** der Schnittstelle Clean ein, und wählen Sie **DTLS Required** aus, wie im Bild gezeigt. Klicken Sie unten auf **Speichern**:



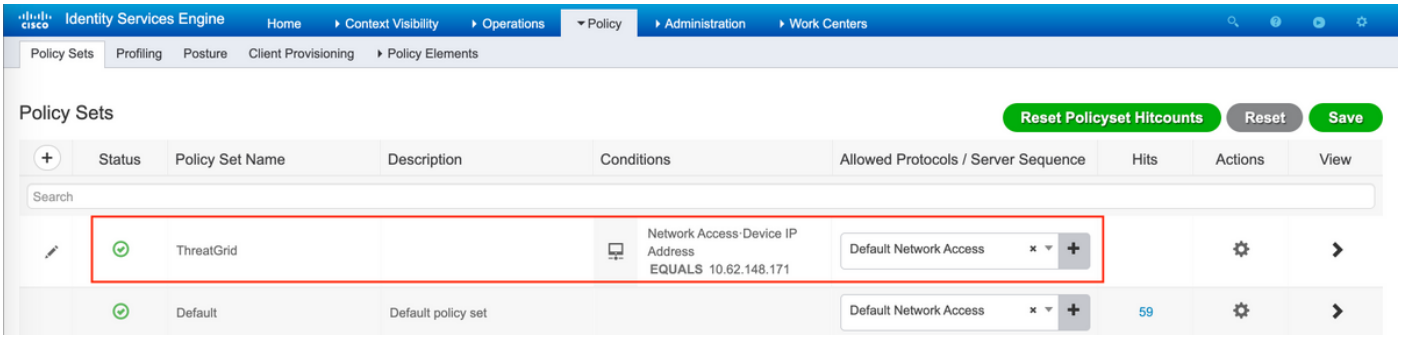

Schritt 4: Erstellen Sie ein Autorisierungsprofil für die Autorisierungsrichtlinie.

Navigieren Sie zu **Richtlinien > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile,** und klicken Sie auf **Hinzufügen**. Geben Sie **Name ein**, wählen Sie **Erweiterte Attributeinstellungen** wie im Bild gezeigt aus, und klicken Sie auf **Speichern**:




Schritt 5: Erstellen Sie eine Authentifizierungsrichtlinie.

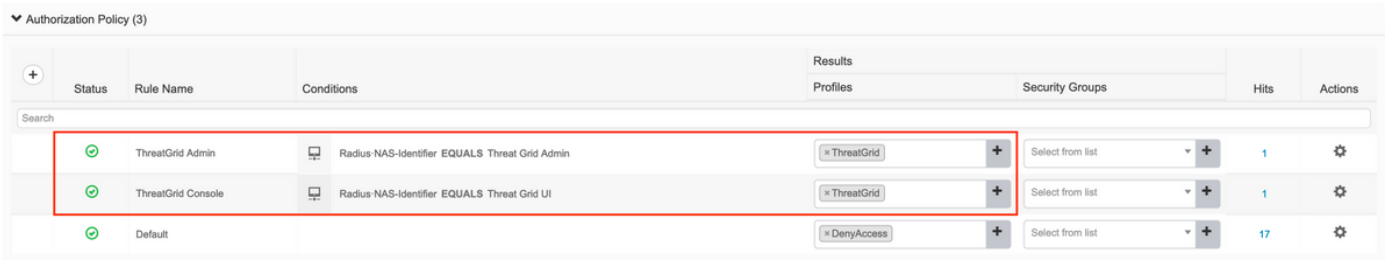
Navigieren Sie zu **Richtlinien > Richtliniensätze**, und klicken Sie auf "**+**". Geben Sie Policy Set **Name** ein, und legen Sie die Bedingung auf **NAD IP Address (IP-Adresse) fest**, die der sauberen Schnittstelle von TG zugewiesen ist. Klicken Sie auf **Save** wie im Bild gezeigt:




Schritt 6: Erstellen Sie eine Autorisierungsrichtlinie.

Klicken Sie auf "**>**", um zur Autorisierungsrichtlinie zu wechseln, erweitern Sie die

Autorisierungsrichtlinie, klicken Sie auf "**+**" und konfigurieren Sie wie im Bild gezeigt, nachdem Sie auf **Speichern** geklickt haben:




> **Tipp**: Sie können eine Autorisierungsregel für alle Benutzer erstellen, die beide Bedingungen erfüllen, Admin und UI.

Schritt 7: Erstellen Sie ein Identitätszertifikat für ThreatGrid.

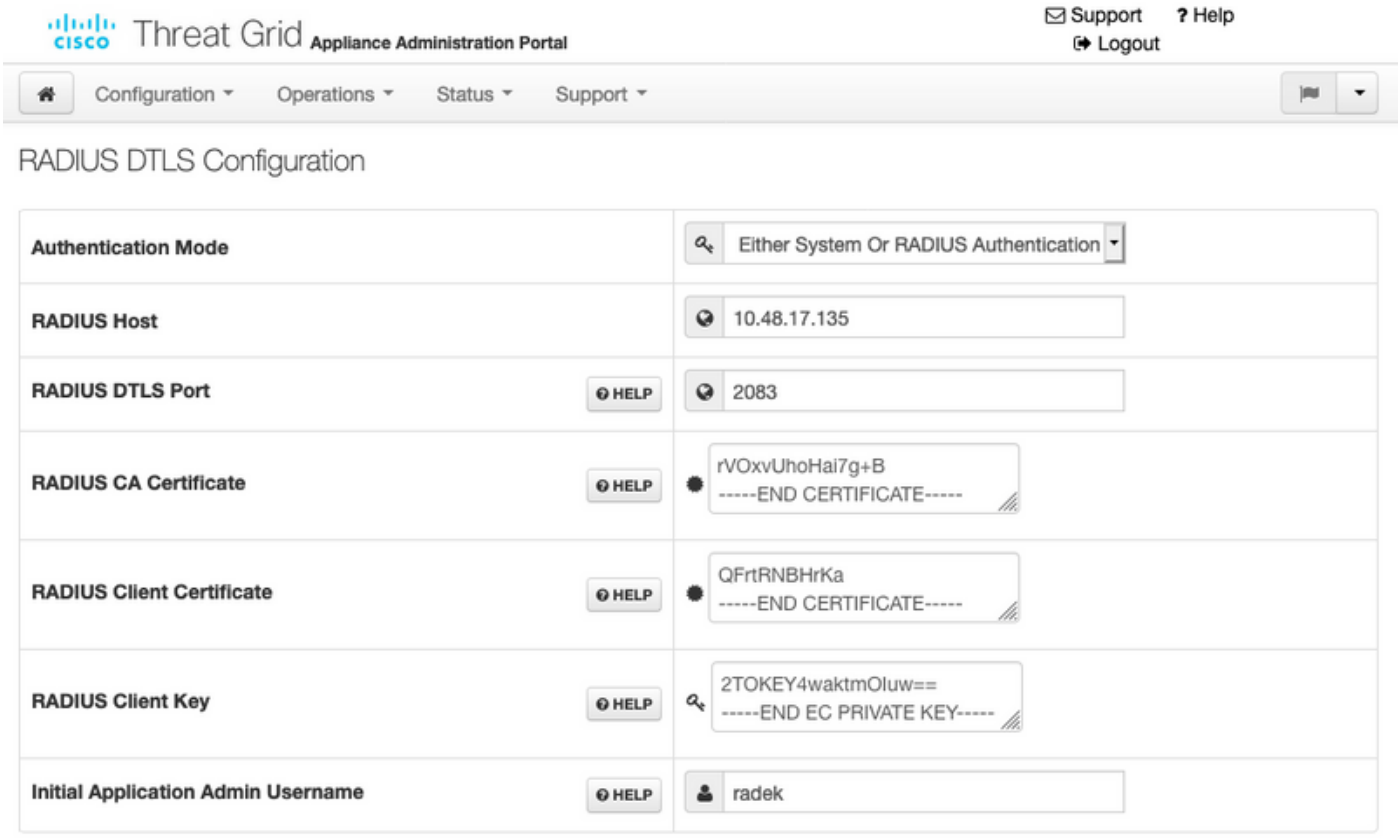
Das Client-Zertifikat von ThreatGrid muss auf dem Elliptic Curve-Schlüssel basieren:

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

Sie muss von der Zertifizierungsstelle signiert werden, der die ISE vertraut. Weitere Informationen zum Hinzufügen *eines Zertifizierungsstellen-Zertifikats zum ISE Trusted Certificate Store* finden Sie unter *Importieren der Stammzertifikate* zur Seite *Trusted Certificate Store*.

Schritt 8: Konfigurieren Sie ThreatGrid für die Verwendung von RADIUS.

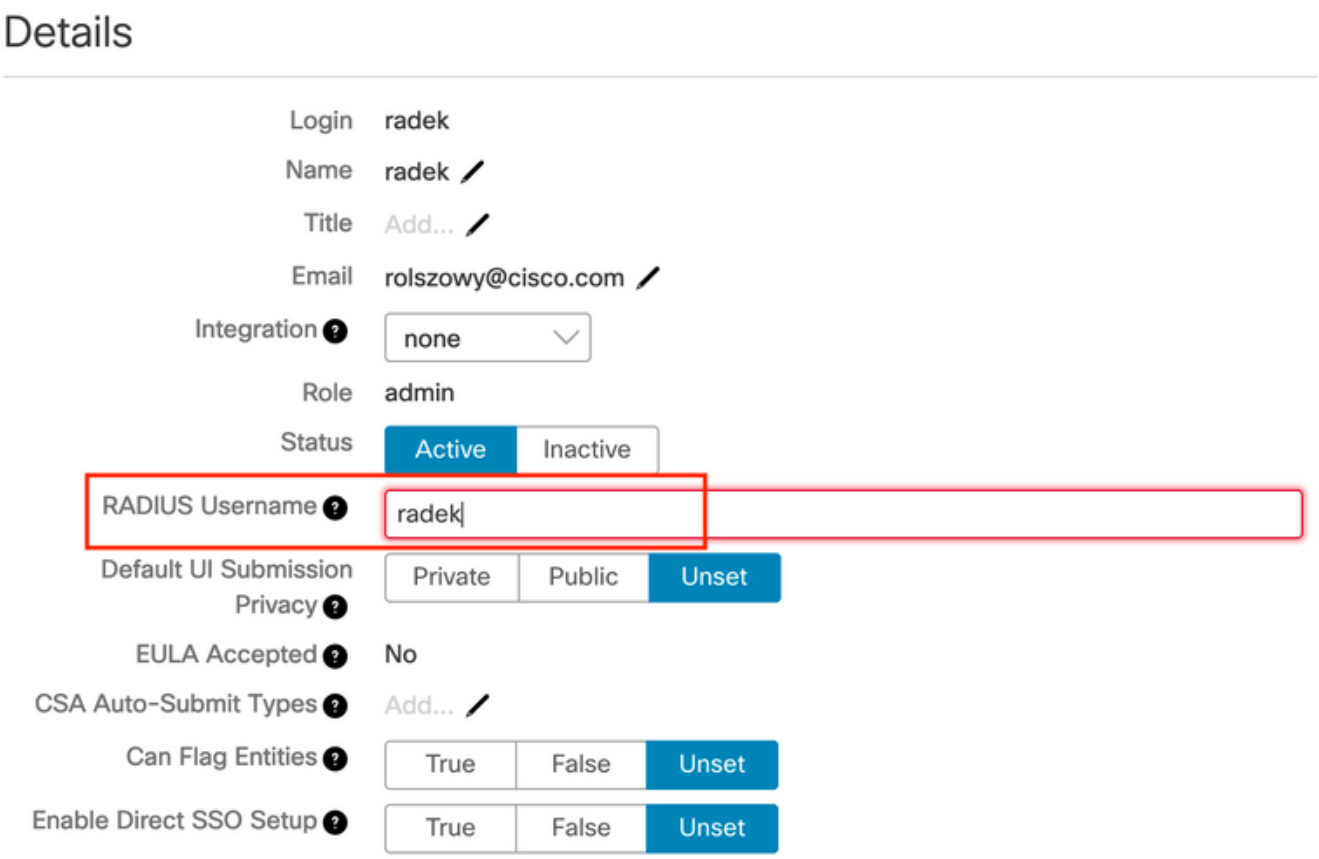
Melden Sie sich beim Admin-Portal an, und navigieren Sie zu **Configuration>RADIUS**. Fügen Sie im RADIUS CA-Zertifikat den Inhalt der von der ISE gesammelten PEM-Datei ein, fügen Sie das PEM-formatierte Zertifikat, das von der CA empfangen wurde, in den Client Key-Paste-Inhalt der Datei private-ec-key.pem aus dem vorherigen Schritt ein, wie im Bild gezeigt. Klicken Sie auf **Speichern**:




> **Hinweis**: Sie müssen die TG-Einheit neu konfigurieren, nachdem Sie die RADIUS-Einstellungen gespeichert haben.

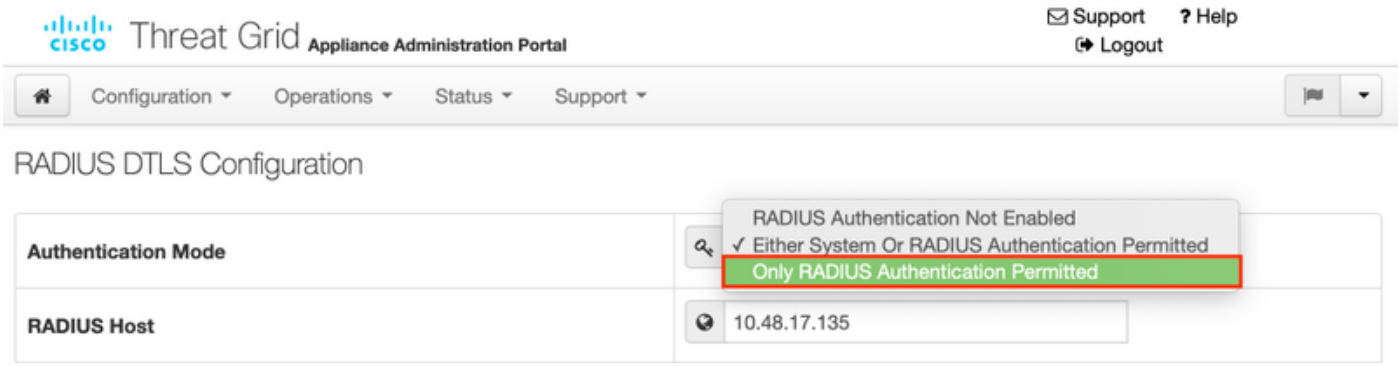
Schritt 9: Fügen Sie den Konsolenbenutzern den RADIUS-Benutzernamen hinzu.

Um sich beim Konsolenportal anzumelden, müssen Sie dem jeweiligen Benutzer das RADIUS-Benutzernamenattribut hinzufügen, wie im folgenden Bild gezeigt:




Schritt 10: Aktivieren Sie nur die RADIUS-Authentifizierung.

Nach erfolgreicher Anmeldung beim Admin-Portal wird eine neue Option angezeigt, die die Authentifizierung des lokalen Systems vollständig deaktiviert und die einzige RADIUS-basierte Option belässt.




# Überprüfen

Nach der Neukonfiguration von TG melden Sie sich ab, und die Anmeldeseiten sehen nun wie im Bild-, Admin- und Konsolenportal aus:


# Authentication Required

Authenticate using RADIUS:

RADIUS Login

RADIUS Password

Authenticate

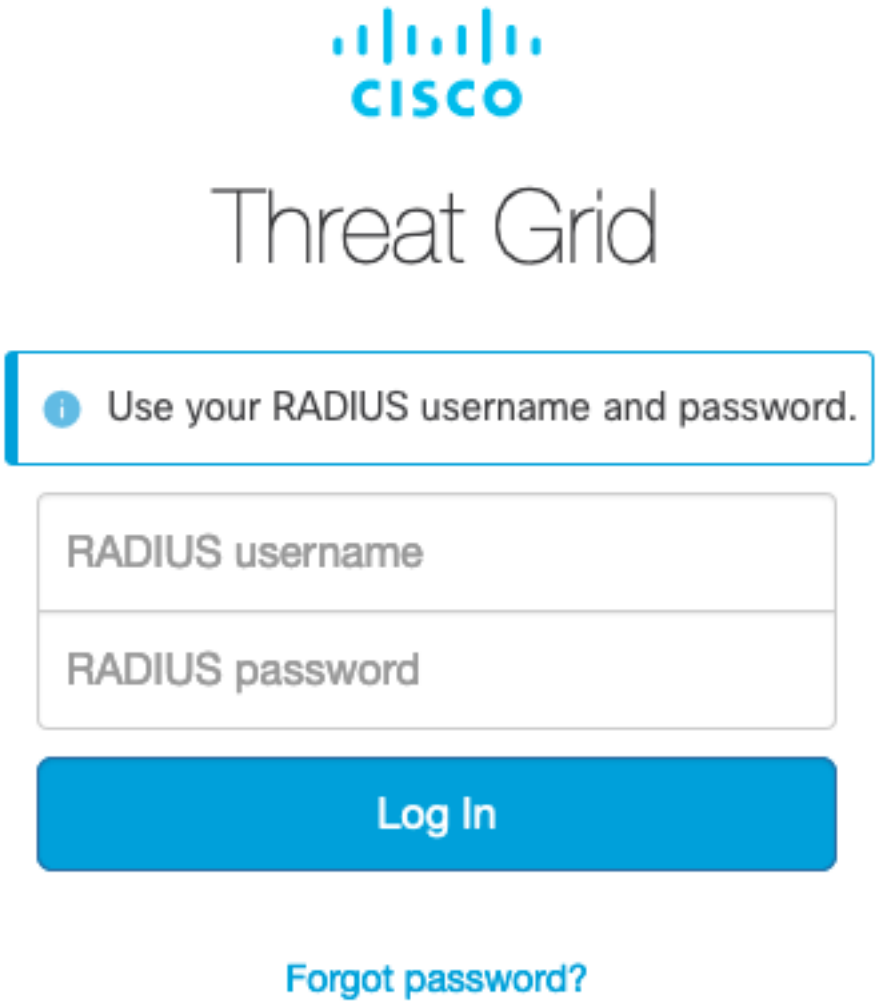
or

Authenticate using System Password:

System Password

Authenticate

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

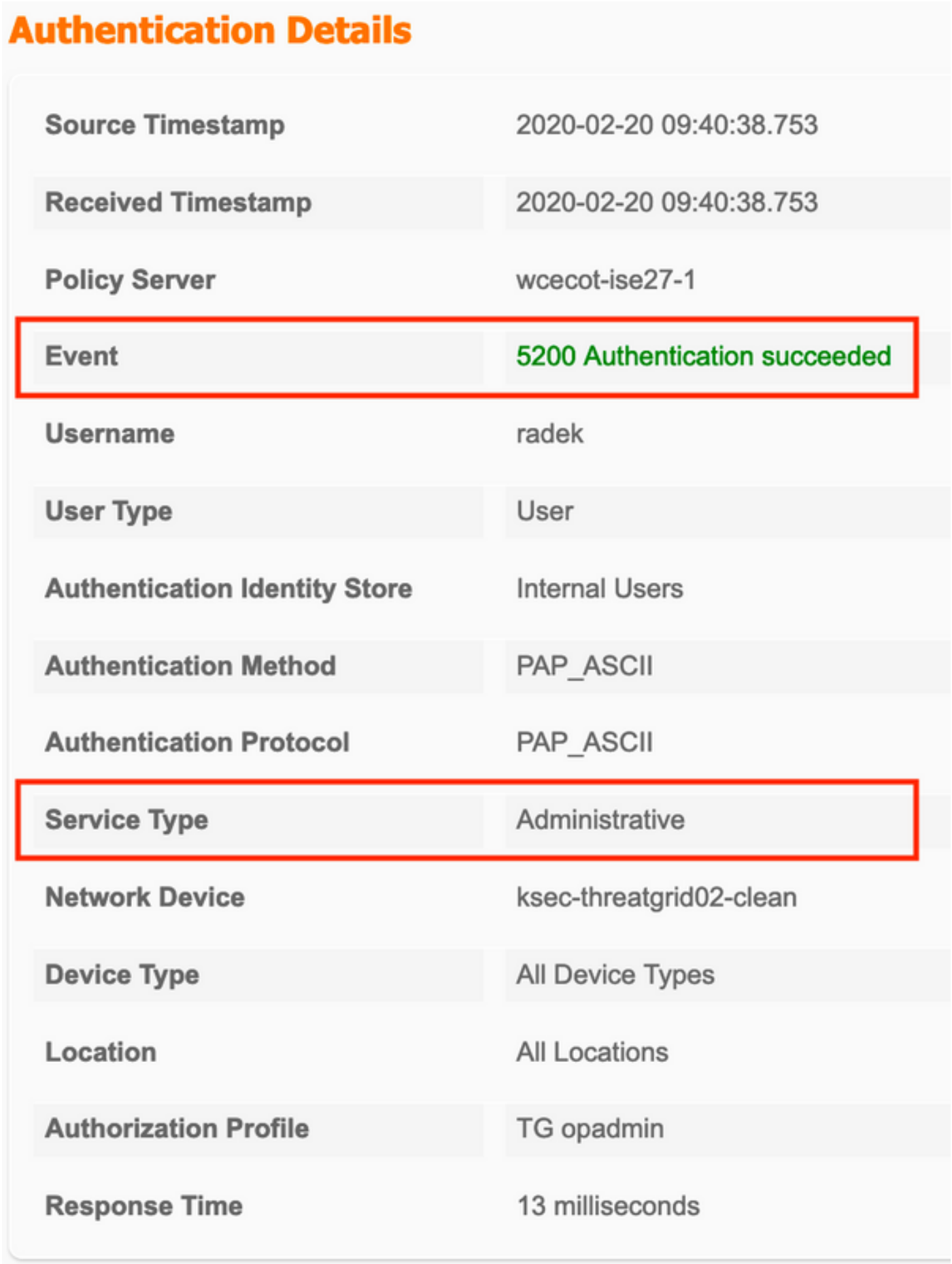



## Fehlerbehebung

Es gibt drei Komponenten, die Probleme verursachen können: ISE, Netzwerkkonnektivität und ThreatGrid.

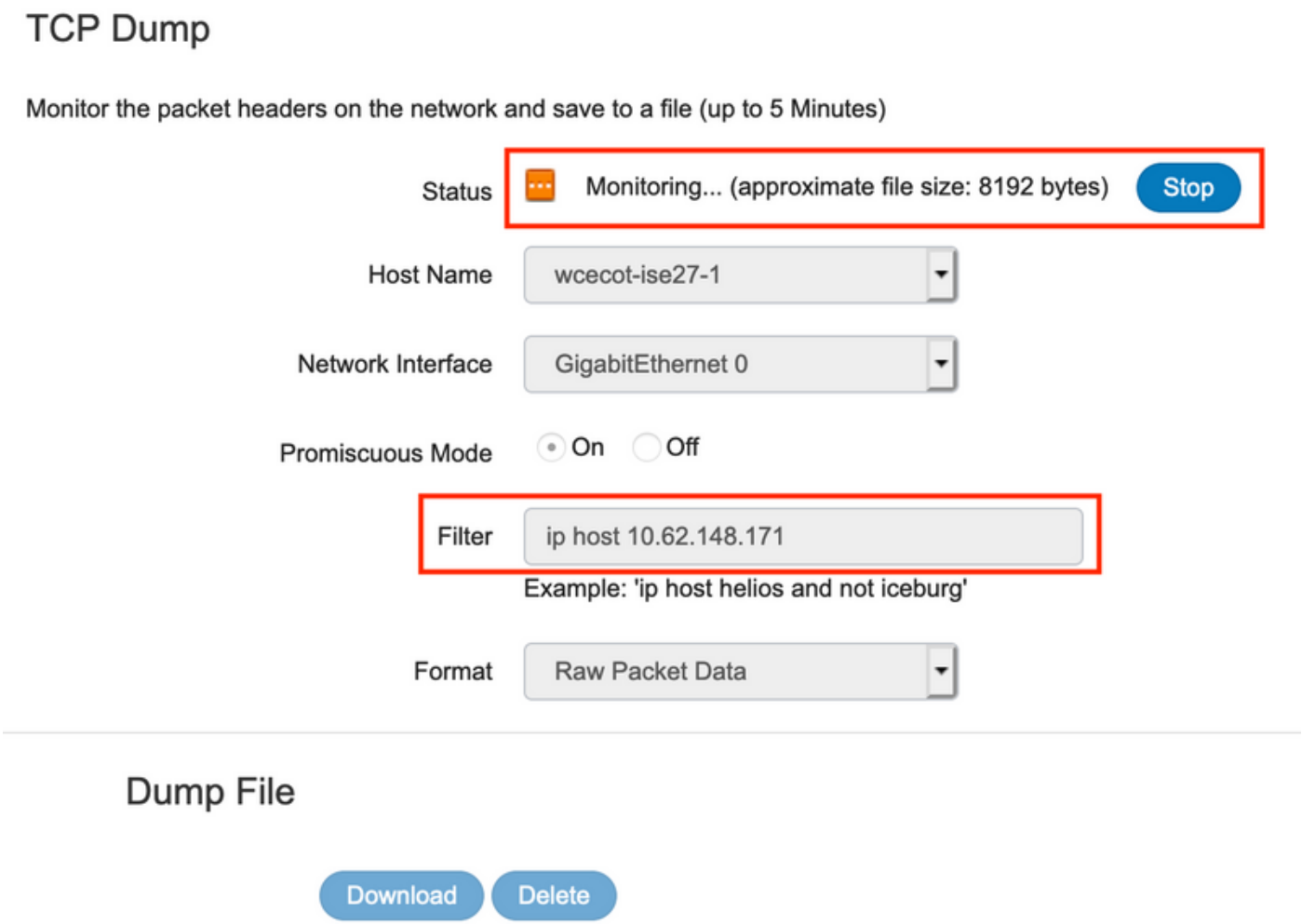
- Stellen Sie in der ISE sicher, dass ServiceType=Administrative an die Authentifizierungsanforderungen von ThreatGrid zurückgegeben wird. Navigieren Sie zu **Operations>RADIUS>Live Logs** auf ISE, und überprüfen Sie die Details:

| 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 |



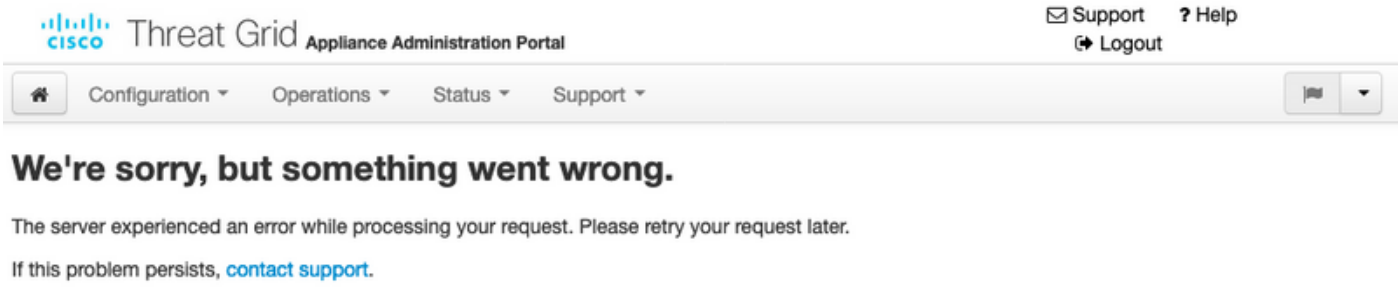

- Wenn Sie diese Anforderungen nicht sehen, erfassen Sie die Pakete auf der ISE. Navigieren Sie zu **Operations>Troubleshoot>Diagnostic>TCP Dump, geben Sie die IP in dem Filterfeld der sauberen Oberfläche der TG ein, klicken Sie auf Start, und versuchen Sie, sich bei**

ThreatGrid anzumelden:




Sie müssen sehen, dass die Anzahl der Byte erhöht wurde. Öffnen Sie pcap-Datei in Wireshark für weitere Informationen.

- Wenn Sie die Fehlermeldung "Es tut uns leid, aber etwas ist schief gelaufen" sehen, nachdem Sie auf Speichern in ThreatGrid klicken, und die Seite sieht wie folgt aus:




Das bedeutet, dass Sie wahrscheinlich den RSA-Schlüssel für das Client-Zertifikat verwendet haben. Sie müssen den ECC-Schlüssel mit den in Schritt 7 angegebenen Parametern verwenden.